LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Businesses Can Fight Surging Email Compromise Scams

By **Jeffrey Rosenthal and David Oberly** (May 1, 2020, 3:54 PM EDT)

Jeffrey Rosenthal

David Oberly

As the novel coronavirus continues to spread across the globe, cyberattacks seeking to exploit the crisis are similarly on the rise.

The frequency of COVID-19 business email compromise schemes — a particularly low-tech, but highly damaging type of cyberscam — has risen significantly in recent weeks, so much so that it prompted the Federal Bureau of Investigation to issue two alerts warning businesses of the growing threat.

As such, businesses must take appropriate measures to effectively mitigate the enhanced risk posed by BEC fraud, which is expected to increase even further in the coming weeks and months.

BEC Scams Explained

BEC scams, also known as CEO fraud and "man-in-the-email scams," involve tricking victims — often those who perform legitimate funds transfers — to make unauthorized wire transfers or send funds directly to the coffers of cybercriminals.

The typical BEC scheme originates with the theft of a corporate executive's credentials by phishing or other means. With those credentials in hand, cybercriminals will then impersonate the executive, sending urgent messages to lower level employees with requests to transfer or wire funds to bank accounts.

According to the FBI's internet crime report[1], the bureau received approximately 24,000 complaints concerning BEC fraud last year, with losses totaling $1.7 billion — accounting for nearly half of all cybercrime-related losses in 2019. While ransomware frequently garners headlines due to the operational disruption caused by these attacks, cybercriminals have had much more financial success with BEC scams, netting at least 17 times more per incident ($75,000) than ransomware ($4,400).

It should come as a no surprise, then, that BEC was far and away the top source of cyber-related financial loss in 2019. BEC fraud is a relatively low-tech and low-cost scam that provides criminals with the ability to focus on high-value targets and high returns, all with minimal risk. This confluence of factors makes BEC scams particularly popular with cybercriminals.

Recent Proliferation of BEC Scams Tied to COVID-19

Over the years, cybercriminals have become more advanced and sophisticated in their attack techniques and methods, leading them to consider the psychological aspect of their scams.

Fraudsters have become extremely adept at exploiting current events — such as terrorist attacks and natural disasters — and the impact on the targets of their scams. As the COVID-19 crisis has deepened over the course of the last month, cybercriminals have adjusted their BEC scams to place a greater emphasis on COVID-19 and enhance the social engineering aspect of their attacks.

For example, BEC fraudsters are impersonating vendors and requesting payment outside the normal course of business, citing reasons relating to COVID-19 for the request. Similarly, cybercriminals claiming to be company executives are emailing lower-level employees requesting urgent, confidential wire transfers to cover costs due to unexpected issues arising from COVID-19.

FBI Issues Back-to-Back Alerts Warning of Anticipated Rise in COVID-19 BEC Schemes

Recently, the FBI issued back-to-back alerts warning of the enhanced threat of COVID-19 BEC schemes.

In its first alert,[2], the FBI warns that cybercriminals are actively exploiting the uncertainty surrounding the COVID-19 pandemic to further the effectiveness of their BEC scams. In particular, the FBI reports that it recently observed a significant spike in BEC fraud targeting organizations purchasing personal protective equipment or other supplies needed in the fight against COVID-19.

The FBI further cautions businesses to anticipate an even greater rise in BEC schemes tied to the COVID-19 pandemic moving forward.

In its second alert,[3] the FBI advises that cybercriminals are targeting organizations that use popular cloud-based email services — i.e., hosted subscription services that enable users to conduct business via tools such as email, shared calendars, online file storage and instant messaging — with an increasing number of BEC scams.

The FBI notes that in doing so, cybercriminals are using tailored phishing kits designed to mimic and impersonate cloud-based email services, making these scams extremely hard to detect as fraudulent.

Moreover, the FBI also reports a troubling trend of cyber criminals accessing the address books of compromised accounts to identify new targets and send phishing emails, allowing a single successful email account compromise at one business to be pivoted to multiple victims within an industry.

Analysis and Risk Mitigation Tips

BEC fraud has continued to grow, evolve and become significantly more sophisticated and deceptive in recent years. As such, BEC scams now represent one of the most destructive types of security threats faced by companies across all industries.

And like many other types of security threats, the prevalence of BEC scams has risen precipitously in recent weeks as the COVID-19 pandemic progresses, with fraudsters aiming to exploit the expanding scope of the crisis.

Moving forward, these same groups will continue to target businesses and individuals with new BEC schemes for the foreseeable future — such as with messaging targeting government stimulus payments set to be disbursed in the coming weeks. Even after the COVID-19 crisis has been put behind us, this type of attack will likely continue to increase, both in frequency and in the extent of losses experienced by victims.

Taken together, those entities that fail to take action to fortify their cyberdefenses against BEC attacks do so at extreme peril. Fortunately, there are several actionable steps businesses can take to mitigate the enhanced risk of BEC scams, including the following:

Cyber and Data Security Policies and Procedures

Businesses should have the proper policies and procedures in place to effectively mitigate the risk of BEC scams and other types of cyberattacks. Often, BEC scams involve the use of deceptive emails designed to appear as though they have originated from a superior or coworker.

Consequently, it is especially important to maintain a detailed corporate communications policy setting forth specific guidelines as to how the company will communicate securely with other members of the organization, which is vital to preventing employees from being tricked into complying with requests from malicious third parties.

Employee Education and Training

Businesses should adequately educate and train their employees on the issue of BEC attacks. Workers should be made aware of the significant threat posed by BEC fraud and the devastating consequences that would result if the company fell victim to an attack of this nature. Businesses should also educate employees on the most common BEC scam scenarios and how to respond in the face of any attempted attacks.

At the same time, businesses should provide workers with tips and best practices to follow to avoid falling victim to these scams, including: (1) exercising vigilance when responding to any last-minute changes in wiring instructions/recipient account information; (2) being cautious of high-level executives making unusual requests and requests from others expressing an abnormal sense of urgency; and (3) checking hyperlinks for misspellings of legitimate domain names or wrong domains (such as an address that should end in ".gov," but which ends in ".com" instead).

Cultivate a Security-First Workforce and Work Culture

Businesses and management should regularly communicate information, tips and tools regarding cyberattacks and cybersecurity generally to all members of their workforce. As vigilance is essential to thwarting BEC attacks, businesses must consistently instill in employees the importance of remaining alert of the ongoing threat of BEC scams — especially during this period when COVID-19 will continue to dominate headlines for the foreseeable future.

Organizations can quickly develop a culture and mindset that maximizes employees' commitment to making cybersecurity a top priority in their day-to-day activities, which in turn can play a significant role in stopping BEC scams and other types of cyberintrusions before they have a chance to wreak havoc on a company's operations and finances.

Utilize Effective Technical Defenses

Organizational defenses against BEC scams often rely exclusively on employees being able to spot attempted attacks as they occur. However, businesses that widen their defenses to encompass more technical measures as an added layer of security can significantly improve their chances of avoiding attempted BEC attacks.

Businesses should implement multifactor password authentication, which prevents cybercriminals from leveraging compromised employee email accounts if their credentials are obtained through phishing attacks or other cybercampaigns.

Maintain an Up-to-Date Incident Response Plan

Finally, businesses should anticipate that a percentage of BEC attacks will prove successful, as planning for these incidents in advance will help minimize any damage caused. Businesses should maintain incident response plans that can be implemented immediately and with adequate resources to respond to an executed BEC scam.

These plans should also be reviewed by key personnel to ensure they are up-to-speed on their roles and responsibilities in the event the plan needs to be put into action.

Conclusion

Businesses must remain vigilant and take proactive steps in defending against the burgeoning security threat posed by BEC scams. At the same time, as cyberthreats continue to develop and evolve at a rapid pace, businesses must also stay current on the latest trends to stay ahead of the curve and effectively defend against these risks, which will remain active and substantial for the duration of the current public health crisis.

To fully manage and mitigate the enhanced risk of BEC scams, businesses should speak with experienced legal counsel to ensure they have the proper policies, procedures and protocols in place to combat these potentially lethal attacks to the greatest extent possible.

And if a business suffers a successful BEC attack or other type of security incident during the COVID-19 crisis (or any time thereafter), experienced counsel should be contacted as soon as possible to provide immediate assistance with rapid response and crisis management, which is key to minimizing the fallout and impact of a breach event.

Jeffrey N. Rosenthal is a partner and David J. Oberly is an associate at Blank Rome LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] FBI, 2019 Internet Crime Report, https://pdf.ic3.gov/2019_IC3Report.pdf.

[2] FBI, FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic, (April 6, 2020), https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic.

[3] FBI, Cyber Criminals Conduct Business Email Compromise Through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion, (April 6, 2020), https://www.ic3.gov/media/2020/200406.aspx.
