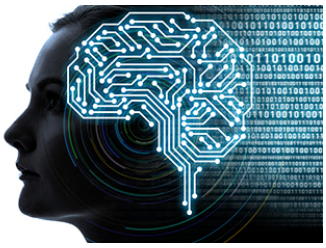

# BEC Compromise - An Update

cyber security  risk management

**Summary:** BEC attacks have cost businesses $26B over the past 4Ys and cybercriminals keep stepping up their game. We share the latest information.

Brain functions happen through connections called synapses. Now, research has shown biological and artificial synapses can happen through the Internet. Technology seems to really allow scientists to step up their game!

Unfortunately, cybercriminals seem to be stepping up their game too, when it comes to targeting businesses. Phishing attacks known as business email compromise (BEC) are so sophisticated that they are 20x more successful than the typical phishing emails sent to consumers.

While many people now know the dangers of clicking on unsolicited links, cybercriminals are tailoring spear-phishing efforts to business employees to make them far less obvious. In BEC attacks, cybercriminals research both companies and the specific employees to make the messages look more realistic. This allows them to bypass traditional email security programs. These attacks have cost businesses more than $26B over the past 4Ys, with an average loss of $270k in the last year, according to a recent report by Barracuda.

Unlike phishing efforts targeting consumers that typically include a link or download, BEC messages instead often mimic legitimate emails. They are almost always sent during business hours from spoofed email addresses or businesses the recipient is familiar with -- sometimes even from legitimate company emails that have been compromised. Eight out of 10 include urgent requests for information, making it more likely for recipients to respond quickly without digging deeper. Cybercriminals also focus more on the time of year these messages are sent, targeting periods when companies usually have lower staffing levels or when employees are likely to be more distracted -- such as tax season or the holidays.

Making it even more difficult, these emails come from high caliber domains or spoofed email addresses from known companies, enabling them to bypass security programs that rely on reputation analysis and blacklists. The most impersonated brands included: Microsoft (32%); Apple (21%); DocuSign (8%); Chase (8%); UPS (7%); Amazon (5%); LinkedIn (5%); American Express (5%); Bank of America (5%) and FedEx (4%).

Given the sly nature of these messages, community financial institutions must be vigilant with their BEC protective processes. Take time to educate employees about these attacks, particularly individuals with access to sensitive data or who are responsible for making payments. You could also employ artificial intelligence scanners that are more likely to identify bogus messages and set up specific account takeover protection measures. You will also want to educate your business customers so that they are aware of these ongoing dangers too.

While this is just a partial list of things to do, we hope we have given you some important information to continue fighting BEC. The technology keeps evolving, so we will be sure to keep you informed as it does.

## OUTSOURCE ALM SERVICES AND REST EASY

Regulators have raised the bar on interest rate risk and liquidity analysis, yet there is more to do than there are hours in a day. To see how easy it is to outsource & get expert help, contact us today.