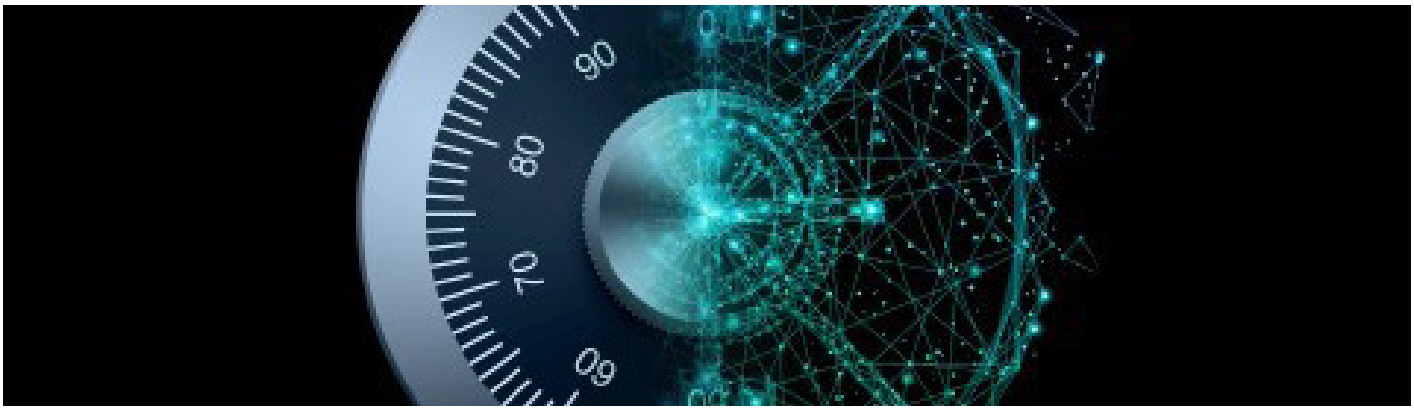
Deloitte.



Focus on Five

Five ways to mitigate the risks of business email compromise attacks

By Rob Biskup and Mike Weil, Managing Directors at Deloitte Financial Advisory Services LLP

In an increasingly common scam known as business email compromise (BEC), cyber thieves are posing as company employees or vendors to commit wire transfer fraud.

BEC exposes firms of all sizes to heavy financial risks and losses. Especially vulnerable are those that regularly carry out transactions with foreign vendors or customers. According to the Federal Bureau of Investigation (FBI), BEC led to adjusted losses of more than $675 million in 2017 alone[1]. More recently, the Securities and Exchange Commission (SEC) issued a rare Report of Investigation to alert companies to BEC and urge them to take enhanced preventive measures[2].

Fraud involving BEC is on the rise as a low-risk, high-reward way to siphon large amounts of cash from victims. Here are five ways organizations can shore up their defenses against this costly threat.

1. Be aware of common BEC attack scenarios.

Criminals often rely on certain tactics to perpetrate BEC scams, including:

A false sense of urgency. Scammers (typically posing as attorneys or executives) send spoof emails to victims and convince them to wire money in support of a business deal, such as an acquisition that the victim's company is undergoing. These emails feign urgency and demand secrecy from the victim.

A trick domain name. In this scenario, victims receive an email asking them to wire money to a specific account. The message originates from a domain that looks credible at first glance, but in fact has been slightly altered (e.g., one character in the domain name is different). These types of attacks exploit the victims' lack of attention to sender details.

Impersonation of a vendor. This type of cyberattack involves electronic communications impersonating one of the company's vendors. The sender's domain name is genuine, and the transaction seems legitimate—often with proper documentation attached—because the scammer has hacked into the vendor's email account. However, the processing details direct payment to an account that the scammer controls.

2. Train employees to recognize BEC attacks.

A fundamental step in safeguarding organizations against BEC is to provide employees with adequate cybersecurity training. Employees should know the risk and implications of these attacks as well as how to respond to an incident. A firm grasp of cybersecurity leading practices can foster a sense of responsibility throughout the organization.

An effective training program emphasizes the central role that grooming plays in these attacks. BEC succeeds not so much because of its technological sophistication, but for its exploitation of human vulnerabilities – including our response to authority. Clear communication of roles and expectations, along with guidance in the appropriate use of IT and accounting controls, can empower employees as the front line of risk mitigation.

3. Create a culture of compliance.

Training alone isn't enough to head off BEC. Scams are constantly evolving, making red flags a challenge to identify. For this reason, training and compliance go hand in hand.

BEC attacks ordinarily target mid-level personnel who seldom communicate with the executives, attorneys, or vendors purportedly behind a transaction request. As a result, employees may not be comfortable with personally approaching the requestor to authenticate the transaction.

An effective compliance culture supports employees with the protocol they need to follow up with confidence. Without the internal isolation BEC criminals depend on, their attacks are more likely to fail.

1 "2017 Internet Crime Report," Federal Bureau of Investigation, https://pdf.ic3.gov/2017_ic3report.pdf.

2 "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements," Release No. 84429, Securities and Exchange Commission, October 16, 2018, https://www.sec.gov/litigation/investreport/34-84429.pdf.

4. Build a layered defense with technical controls.

For all its psychological manipulation, BEC is not necessarily sophisticated from a technical standpoint. Most BEC attacks originate from spear phishing or spoofing an internal email account. They can be prevented or detected via IT controls such as application-based multi-factor authentication (MFA) and virtual private networks (VPNs).

Another effective anti-BEC approach is to use encryption to authenticate emails and allow users to safely exchange data. Encryption software translates the data into a code for transmitting over a network. The transmission is unintelligible without a "public key" to decrypt the data.

5. Optimize accounting systems and controls.

Now that most corporate financial transactions are digital, financial crime from cyber fraud is poised to reach epidemic levels. That has prompted the SEC to weigh in. In its October 2018 report, the SEC declined to recommend enforcement against companies that experienced losses due to inadequate controls. At the same time, however, the agency offers a pointed warning to public companies in general: Consider the risks of cyber-related fraud and reassess internal controls accordingly.

By mapping the existing workflow for wire transfers, organizations can analyze their processes to identify potential weaknesses and enhancement opportunities. An example of an enhancement opportunity is the enforcement of limits on the amount of money each executive can approve. Another is the implementation of authorization of wire transfers, including a protocol for approvals when senior executives are the initiators of these transactions.

Our take:

BEC is a criminal phenomenon with potentially severe consequences. More likely than not, these types of attacks will continue to rise, both in frequency and losses to the companies that fall victim.

The majority of BEC criminals live and operate outside of the United States, making it difficult for law enforcement to prosecute them. As a result, prevention and detection are an imperative. Now is the time for companies to educate themselves about BEC, train their employees, and create an environment that encourages compliance. Together with hardened networks and optimized controls, these measures provide organizations with the advantage they need to keep BEC at bay.

In a June 2017 Public Service Announcement, the FBI offered these additional tips for mitigating BEC attacks:

- Frequently monitor your email exchange server for changes in configuration and custom rules for specific accounts
- Consider adding an email banner stating when an email comes from outside your organization so they are easily noticed
- Conduct end user education and training on the BEC threat and how to identify a spear phishing email
- Ensure company policies provide for verification of any changes to existing invoices, bank deposit information, and contact information
- Contact requestors by phone before complying with e-mail requests for payments or personnel records
- Consider requiring two parties sign off on payment transfers[3]

3 "Business email compromise contributes to large scale business losses nationwide," Alert Number I-061118-PSA, Public Service Announcement, Federal Bureau of Investigation, June 11, 2018, https://www.ic3.gov/media/2018/180611.aspx.

Let's talk.

Rob Biskup
Managing Director | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1.313.396.3310
rbiskup@deloitte.com

Michael Weil
Managing Director | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 312 486 0207
miweil@deloitte.com

Deloitte.