EXPOSING BUSINESS EMAIL COMPROMISE:

How Fraudsters Infiltrate Trusted Relationships

By **Sheree Mann**, CPA, CA, CBV, CFI, CFF
Managing Director, Delta Consulting Group

IT STARTED WITH A SIMPLE EMAIL – AND ENDED WITH A $670,000 LOSS.

Business email compromise, also known as BEC, is not just a theoretical cyberthreat. It is a growing and costly reality impacting public and private organizations across the globe. Entities in every sector and industry are being targeted by BEC scammers. While there are different means that a BEC scammer can use to execute a BEC, the end game is always the same, to convincingly request fraudulent and unauthorized funds transfers. In one recent case, fraudsters successfully diverted hundreds of thousands of dollars from a government entity by impersonating a trusted vendor and manipulating standard payment procedures.

Organized groups of fraud scammers are focused on BEC as their preferred method of fraud scam as it is extremely lucrative. Local businesses, large corporations, government entities and individuals are all being targeted.

Small and medium sized businesses are often more vulnerable because they typically have high trust cultures, fewer internal controls, a lack of employee training and limited cybersecurity resources. Larger businesses are also susceptible. In 2017, Google and Facebook lost more than $100 million USD to a fraud threat group using a BEC phishing scheme. Using fake email accounts, designed to mimic employee accounts of a purported business partner, phishing emails with fake invoices were sent to employees who “regularly conducted multi-million-dollar transactions” with the purported business partner. The targeted employees responded by paying out more than $100 million to a fake company’s bank accounts.

In 2024, reports revealed a sharp rise in compromised employee-linked accounts across Fortune 500 companies, with more than three million accounts exposed between 2022 and 2024. This trend highlights the significant risks posed by leaked credentials, which can enable account takeovers, business email compromise scams, fraud and data breaches.

Awareness is key. Training is essential.

If your company has never been the target of a BEC, it is helpful to understand the typical trajectory of a BEC scheme. In this article, we break down how one construction company and government entity fell victim to a targeted BEC attack and offer tips and resources to help you reduce your organization's exposure.

A CLOSER LOOK: FRAUDSTERS SCAM $670,000 FROM A GOVERNMENT ENTITY

In 2024 an accounts payable clerk for a government entity responded to a purported vendor's email request to change its bank account information. After the clerk completed the bank account change, payments of approximately $670,000 were processed and diverted to a non-vendor bank account.

The vendor account targeted in this incident was a construction company that was an established vendor of record for the government entity.

HOW DID THE BUSINESS EMAIL COMPROMISE OCCUR?

The fraudsters committed the crime by attempting to conceal their identity by:

1) **Creating a fake domain** that was very similar to the vendor's domain. In fact, an uppercase "i" (I) was substituted for a lower case "L" (l) in the domain name to conceal the identity of the fraudster. The scammer impersonated the account receivable clerk of the construction vendor in email communications with the accounts payable clerk of the government entity and requested a change to the bank account.
2) **Including fictitious documents** in emails sent to the government entity to support the alleged bank account change made by the vendor.
3) **Copying a more senior government employee** in the compromised email sent to the accounts payable clerk to provide credibility to the compromised email.

HOW WAS THE FRAUD IDENTIFIED?

After the initial breach, the fraudster also sent an additional email that included a fictitious invoice for $320,000 for an apparent outstanding account and requested immediate payment. The email raised questions about the vendor account and the clerk reached out to the construction company by phone. As a result, the BEC scheme was discovered.

The bank was immediately notified, and the construction company launched a cyber incident investigation. At the same time, the government entity hired external legal counsel and a forensic accountant and launched its own investigation. The incident was also reported to the police.

To recover the transferred funds, the government entity filed a statement of claim against the bank and recovered $240,000 that remained in the scammer's bank account. Forensic accountants traced the remaining funds disbursed from the scammer's bank account to other accounts, which revealed that the remaining funds were dissipated by the fraudster and no further assets were identified for recovery purposes

BEST PRACTICES FOR REDUCING BEC RISK

An informed and engaged workforce is crucial to preventing losses from BEC, and other frauds and cybercrimes.

1) Educate employees to increase their recognition of phishing schemes. Use training sessions to increase employee's awareness of red flags involved in BEC schemes, provide current real-life examples, and simulate relevant phishing attacks used by fraudsters.
2) Train employees on ways to validate the legitimacy of email addresses and email requests for and/ or changes to sensitive information (such as bank accounts).
3) Heighten employees' awareness of the risk in situations that require urgent actions, immediate payments, or bank account changes.
4) Develop and enforce protocols to process urgent vendor requests requiring immediate actions, payments, or account changes. These protocols should include a secondary channel or verbal verification procedure by an existing phone number (not based on email information) for urgent requests and account changes.
5) Ensure the use of security software to assist in detecting phishing attacks.

HOW CAN A FORENSIC INVESTIGATOR HELP?

Forensic investigators and accountants play a vital role in helping entities prevent and manage frauds and scams like BEC. These specialized professionals conduct detailed investigations to gather financial facts and evidence, review internal controls and vendor data management systems to identify weaknesses / vulnerabilities and provide recommendations to improve systems to assist in the prevention and deterrence of future potential fraud incidents. In the aftermath of an incident, they work as part of the investigation team to identify the fraudsters, trace funds, identify the perpetrator's assets and support the recovery efforts. Forensic accountants often prepare expert reports for insurance claims, civil proceedings and for purposes of reporting incidents to the police, ensuring all findings are documented and defensible. They also deliver targeted employee training to raise awareness of BEC tactics, helping staff recognize red flags and reduce the likelihood of future risks of BEC attacks and exposure.

There is no time like the present to take inventory of your vulnerabilities, especially as they relate to business email compromise, a prevalent area of fraud. Click here to download a one-page guide that will help you identify common risk factors that could put your entity in jeopardy.

ABOUT THE AUTHOR

SHEREE MANN, CPA, CA, CFF, CBV, CFI

MANAGING DIRECTOR

T: +1 (416) 926 4217 E: smann@delta-cgi.com

Sheree Mann, Managing Director of Delta Consulting Group Canada Ltd. has more than 30 years of exclusive experience in financial and fraud investigations, forensic accounting and quantifying economic losses in criminal and civil matters. She has investigated financial allegations related to public and private companies, unions, charities, government agencies, municipalities, and individuals. Sheree has provided expert testimony in criminal and civil court and a public inquiry.