Quick Guide: Tips on Safeguarding Your Bank and Customers from Business Email Compromise

What is Business Email Compromise?

"Business Email Compromise" (BEC) is a sophisticated scam which targets both businesses and individuals performing wire transfer payments or other means of electronic fund transfers (EFTs).

BEC "Red Flags"

- An urgent email requesting that a wire transfer be sent immediately
- The email domain name is very similar to the legitimate domain
- The content of the email reflects transaction:
  - Instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used.
  - Seems legitimate, but contain different language, timing, and amounts than previously verified and authentic transaction instructions.
  - Originates from an email account closely resembling a known customer's email account; however, the e-mail address has been slightly altered by adding, changing, or deleting one or more characters.
  - The email contains incorrect grammar and/or syntax.
  - Directs payment to a beneficiary with which the customer has no payment history or documented business relationship, and the payment is in an amount similar to or in excess of payments sent to beneficiaries whom the customer has historically paid.
  - Requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors.
- Position of the sender.
- An observable change in email traffic deleted or missing emails.

Technical Solutions

- Multi-factor Authentication.
- Behavioral analytics.
- Anti-Phishing:
  - White/blacklisting.
  - Domain-Based Message Authentication, Reporting & Conformance (DMARC).
- Information sharing.
  Monitor email settings for unauthorized auto-forwarding rules or filter settings.

Operational Controls

- Internal and operational controls:
  - Dual custody and separation of duties for critical payment transaction processing and accounting tasks.
  - Payment data verification.
  - Clear error processing and problem resolution procedures.
  - Confidential and tamper-resistant mailing procedures for bankcards and other sensitive material.
- Risk assessments.
- Work with bank's treasury management group to create ACH blocks and filters.
- Loss prevention consulting.
- Regular audits.

Training and Awareness

- Annual and new hire fraud training.
- Provide employee and customer fraud/security awareness training material.
- Provide security manuals that accompany.
- Provide a commercial customer security newsletter.

Recovering the Funds

1. Document actions related to the incident as they occur for evidentiary purposes then filing a report with law enforcement.
2. Follow SWIFT's wire transfer recall process.
3. Prepare and have the victim organizations legal documentation signed and available to be sent to the recipient wire transfer institution (e.g. Unauthorized Electronic Fund Transfer Affidavit of Fraud and Hold Harmless or Letter of Indemnity).
4. Identify fraud counterpart and notify them of the fraud.
5. Provide legal document to correspondent institution.
6. Monitor and follow-up.

Incident Reporting

- Notify regulator and law enforcement.
- Locate your local FBI or USSS field office, or file a complaint online at www.IC3.gov.
- Submit a Suspicious Activity Report (SAR) utilizing the BEC term to make it easier for law enforcement to track.
- Report any observed fraudulent activity through a trusted information sharing organization like FS-ISAC.

Building Your Incident Response Program

Protecting your business against a BEC incident is the best way of avoiding financial loss. Being prepared to respond a BEC incident will enable your business to limit the damage in the event a threat actor is successful.

Using the below outline incorporate a BEC scenario into your existing Incident Response Plan (IRP) provides you with a better chance of reducing or recovering lost monies and provides ongoing business resiliency.

1. Prepare and Plan:
   - Develop your plan - Identify how you will respond to a BEC incident.
   - Obtain leadership support.
   - Test the effectiveness of your plan.
   - Identify members of your incident response team.
   - Provide all aspects of your IRP (training, execution, hardware and software resources, etc.) to your IRP team.
2. Detection and Analysis:
   - Determine what happened, how it was discovered, what areas have been impacted, what is the potential loss amount, which departments are affected, have you isolated the account(s) and institution(s) involved?
3. Containment, Eradication, and Recovery:
   - Make sure no other accounts are involved with the incident – if there are, prevent the funds from being transferred.
   - Communicate with internal departments and prevent other points of compromise.
   - Implement steps to recover the funds.
   - Notify your regulator and law enforcement.
4. Review and Update Plan:
   - Revisit the incident and document what happened and how, develop and incorporate new controls, revise your IRP.
   - Update technical solutions your bank is using if there are one or more gaps in your loss prevention strategy.