Incident Response Playbook: Business Email Compromise (BEC)

Team AnubisX

Version 1.0
September 17, 2025

Document Control

Attribute	Value
Version	1.0
Status	Final
Owner	AnubisX Security Team
Review Cycle	Every Quarter

Contents

1 Introduction

1.1 Purpose

The purpose of this playbook is to provide a clear incident response plan for handling Business Email Compromise (BEC) incidents, with the objective of minimizing financial loss, ensuring business continuity, and preventing recurrence.

1.2 Scope

This playbook applies to all systems, networks, email accounts, finance processes, and employees within the organization. It covers all stages of incident response, from preparation to post-incident lessons learned.

2 Overview of Business Email Compromise

Business Email Compromise (BEC) is a targeted email scam where attackers impersonate executives, vendors, or partners to trick employees — often in finance or HR — into making wire transfers, sending sensitive information, or changing payment details. BEC typically involves social engineering, email account takeover, or domain spoofing and can result in significant financial and reputational damage.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure the team is equipped and ready to respond to a BEC incident before it occurs.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensic Analyst, Communications Lead, Finance Liaison).
- **Tools & Resources:** Ensure availability of email gateway filters, EDR, SIEM, secure communication channels, and fraud monitoring tools.
- **Training:** Regular BEC awareness training for finance, HR, and executives; simulated BEC drills.
- **Financial Controls:** Implement wire-transfer verification procedures (dual-approval), vendor payment validation, and hold periods for large transfers.
- **Contact Lists:** Maintain updated contacts for banks, payment processors, legal counsel, and law enforcement (e.g., local cybercrime units).
- **Threat Intelligence:** Monitor BEC TTPs, lookalike domains, and reported scams relevant to the industry.

3.2 Phase 2: Identification & Analysis

Goal: To confirm BEC activity and determine its scope and severity.

1. **Initial Triage:** Collect reports from employees or automated alerts, preserve email headers and messages, open an incident ticket, and activate secure communications.

2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
   - **Email:** Unusual sender addresses, spoofed domains, reply-chain anomalies, newly added mailbox forwarding rules.
   - **Transaction:** Unapproved wire transfer requests, changed payment details, requests for urgent/secret transactions.
   - **Account:** Account takeover signs (unusual logins, MFA bypass attempts), mailbox rule creation, or auto-forwarding.
3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on the financial impact, data exposure, and scope of the compromise.

Level	Description	Example	MTTD	MTTR
Level	**Description**	**Example**	**MTTD**	**MTTR**
Low	A single suspicious BEC email detected, no interaction or financial loss.	An employee receives an invoice email from a spoofed vendor domain and reports it to security without action.	1-6 hours	24 hours
Medium	User interacted or minor unauthorized change detected; no confirmed financial loss.	An employee replied to a spoofed CEO email, but finance flagged the request before transfer.	6-24 hours	1-3 days
High	Successful unauthorized transfer or multiple accounts compromised.	A vendor change request was acted upon, and a wire transfer was sent to a fraudulent account.	24-48 hours	3-7 days
Critical	Large-scale fraud, executive impersonation, with major financial or regulatory impact.	BEC leads to multiple high-value unauthorized transfers, payroll diversion, or sensitive data exposure.	48 hours	7-14+ days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious activity with other data points and BEC-specific threat intelligence.
   - **If True Positive (TP):** The activity is confirmed as BEC. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the BEC playbook.
   - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and recommend tuning detection rules.
5. **Incident Declaration:** If confirmed, formally declare a BEC incident and escalate to leadership, finance, and legal teams.

3.3 Phase 3: Containment

Goal: To stop the financial loss and prevent further unauthorized activity.

- **Short-Term Containment (Immediate Actions):**
  - Immediately contact banks/payment processors to attempt recovery or freeze funds.
  - Suspend affected email accounts and revoke all active sessions.
  - Quarantine related emails and block spoofed/suspicious domains.
- **Evidence Preservation:** Preserve email headers, transaction logs, and login records **before** remediation.
- **Long-Term Containment Strategy:** Implement emergency financial controls (e.g., hold all wire transfers, verify all recipient changes).

3.4 Phase 4: Eradication

Goal: To remove attacker artifacts and close security gaps.

- **Root Cause Analysis:** Identify the method of compromise (e.g., phishing, account takeover).
- **Account Remediation:** Remove malicious mailbox rules. Revoke and rotate compromised credentials; enforce MFA.
- **System Remediation:** Reimage compromised endpoints if malware is present.
- **Security Hardening:** Patch and harden systems involved in the compromise.

3.5 Phase 5: Recovery

Goal: To safely restore normal operations and recover funds.

- **System Restoration:** Work with banking partners to attempt fund recovery. Restore mailboxes and validate account integrity.
- **Enhanced Monitoring:** Increase monitoring for suspicious email and financial activity post-restoration.
- **Validation:** Ensure all malicious access is removed before returning accounts to normal use.
- **Business Continuity:** Resume normal financial operations with enhanced verification procedures for a set period.

3.6 Phase 6: Post-Incident Activities (Lessons Learned)

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem with finance, legal, and leadership.
- **Final Incident Report:** Prepare a detailed report including timelines, financial impact, and recovery actions.
- **Action Plan:** Implement stronger controls like mandatory dual-approval, out-of-band verification for payment changes, and full DMARC/DKIM/SPF enforcement.

4 MITRE ATT&CK Framework Mapping

Business Email Compromise (BEC) ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1566 – Phishing*
  - *T1078 – Valid Accounts*
  - *T1133 – External Remote Services*
- **Tactic: Persistence**
  - *T1098 – Account Manipulation:* Creating forwarding rules.
  - *T1136 – Create Account*
- **Tactic: Credential Access**
  - *T1110 – Brute Force*
  - *T1606 – Forge Web Credentials*
- **Tactic: Discovery**
  - *T1114 – Email Collection*
  - *T1069 – Permission Groups Discovery*
- **Tactic: Impact**
  - *Financial Theft:* Direct impact through fraudulent transfers.