Business Email Compromise Response and Prevention Guide

Table of Contents

This guide provides general information and should be adapted to the organization's environment, contractual commitments and applicable laws. It is not a substitute for advice from legal counsel, the cyber-risk insurer or relevant authorities.

argus TECHNOLOGY

Introduction

Business email compromise can begin with a single deceptive message and develop into financial fraud, unauthorized disclosure of information, credential theft or access to connected systems. A successful response therefore requires more than resetting a password. Leadership, legal, insurance, communications, finance and technical teams may all have actions to take.

This guide describes the common features of BEC, the actions an organization should consider after discovery, and the controls that can reduce the likelihood and impact of recurrence. It is intended for organizations of different sizes and should be used alongside the organization's incident-response plan.

1. Understanding Business Email Compromise

Business email compromise, commonly shortened to BEC, is a form of fraud in which a criminal uses email or a trusted digital identity to make a request appear legitimate. The attacker may take control of a real mailbox, imitate a familiar address or domain, or use information from earlier conversations to make the request convincing.

Although payment fraud is a common objective, BEC can also be used to obtain payroll information, tax records, customer data, passwords, documents or access to other business systems.

1.1 How BEC typically occurs

- **Credential phishing —** A user is directed to a false sign-in page, allowing the attacker to capture a password, session or authentication approval.
- **Mailbox takeover —** The attacker signs in to a legitimate account, studies existing conversations and sends messages from the trusted mailbox.
- **Domain or address impersonation —** A look-alike domain, display name or slightly altered address is used without compromising the real account.
- **Conversation hijacking —** The attacker joins or recreates a genuine email thread and changes payment details, delivery instructions or contact information.
- **Malware or token theft —** Malicious software, stolen browser sessions or unauthorized applications provide access even when the password itself is not known.

1.2 Common warning signs

- Unexpected MFA prompts, unfamiliar sign-ins or unexplained changes to passwords, recovery details or authentication methods.
- New forwarding, inbox, deletion or concealment rules that the mailbox owner does not recognize.
- Urgent or confidential requests involving payments, payroll, gift cards, tax information, credentials or changes to bank details.
- Messages that use a familiar name but a different address, domain, reply-to address or writing style.
- A supplier, customer or employee reports receiving a message that the apparent sender did not send.
- Requests to avoid normal approval steps, change communication channels or keep the transaction secret.

2. Immediate Leadership and Communication Actions

Communication is an incident-response workstream, not an activity to address after the technical investigation. Early messages can affect financial recovery, contractual relationships, legal obligations, insurance coverage

and the organization's reputation. The response should therefore be led through an agreed structure from the beginning.

2.1 Establish control

- Assign one Incident Lead with authority to coordinate decisions, establish priorities and maintain the incident timeline.
- Use a trusted communication channel. Do not coordinate through a mailbox that may still be compromised.
- Engage legal counsel and the cyber-risk insurer promptly. Review the policy for notification deadlines, consent requirements, approved service providers and coverage conditions.
- Bring in Finance, Privacy, Communications, Human Resources and operational owners according to the suspected impact.
- Record confirmed facts, assumptions, decisions, owners and the time of the next update. Avoid waiting for complete certainty before taking time-sensitive protective action.

2.2 Plan and control communications

- **Set an approval route —** Decide who may approve and issue messages to employees, customers, suppliers, regulators, banks, insurers, law enforcement and the media.
- **Route inquiries —** IT staff and other employees should direct requests for information to management or the designated communications contact. Premature or unapproved statements about an incident may create legal, contractual, or reputational risk.
- **Use confirmed facts —** Separate what is known from what is still being investigated. Do not speculate about cause, attribution, financial recovery or the scope of affected information.
- **Give useful instructions —** When notification is appropriate, identify the affected message or action, explain what the recipient should avoid or verify, provide a trusted contact point and state when the next update is expected.
- **Keep a record —** Retain the approved wording, recipients, communication channel, time sent and responses received.

2.3 Financial and law-enforcement response

If money may have been transferred, Finance should contact its financial institution immediately to request a hold, recall or freeze and ask the bank to contact the receiving institution. This should not wait for the technical investigation to finish.

- Use trusted, previously held contact details to verify the bank, supplier, customer or employee involved.
- Record the amount, currency, time, beneficiary, account details, payment reference and approval path, and preserve related invoices and messages.
- Contact the local FBI field office as appropriate and file a report with the Internet Crime Complaint Center at ic3.gov.
- Coordinate the timing and content of reports with legal counsel, the insurer and financial institutions where appropriate. Reporting requirements and recovery options vary by applicable federal and state law and the circumstances.

2.4 Legal and regulatory considerations

Legal counsel should assess whether the incident may trigger privacy, breach-notification, contractual, employment, regulatory or litigation obligations. The assessment should consider what information was accessed or disclosed, the individuals and states involved, notification deadlines, customer contracts and any commitments made to the insurer.

Preserve relevant records and follow counsel's direction on investigation reporting and communications. Technical findings should be accurate and complete, but they should not be distributed more widely than necessary before the organization has agreed how sensitive incident information will be handled.

3. Technical Containment and Investigation

Containment and investigation normally begin together. One workstream stops further misuse while the other preserves evidence, establishes the likely time window and determines whether the attacker reached people, information or systems beyond the mailbox.

3.1 Containment

- **Secure the identity —** Restrict sign-in, reset the password through a trusted administrator session and identify other accounts where the same or a similar credential may have been used.
- **Revoke access —** End active sessions, revoke available refresh tokens and verify MFA and recovery methods. Remove anything the user or administrator cannot confirm.
- **Remove persistence —** Record suspicious settings before removal, then review forwarding addresses, inbox and deletion rules, delegates, mailbox permissions and application consent.
- **Inspect the endpoint —** Review the device used during the relevant period. Isolate it when malware, session theft or continued attacker activity is suspected.
- **Limit connected access —** Temporarily restrict affected cloud, VPN, administrative or client-system access when the account may provide a path beyond email.

3.2 Investigation

- **Preserve evidence —** Retain original messages and headers, audit and sign-in records, message traces, relevant endpoint alerts, screenshots and timestamps. Evidence collection should not delay urgent containment.
- **Review authentication —** Check IP addresses, locations, devices, applications, authentication results, MFA events and identity changes. Start with the earliest reliable indicator and widen the review period when necessary.
- **Review mailbox activity —** Examine sent, deleted and draft items, message trace, forwarding, rules, delegates and permissions. Identify recipients, replies, links, attachments and instructions issued from the account.
- **Check wider exposure —** Review collaboration and file services, password stores, remote-support tools, cloud platforms, VPN access and other systems available to the user.
- **Search related accounts —** Look for the same indicators, recipients, infrastructure or methods in other accounts where the evidence supports a wider search.

3.3 Establishing scope

The initial scope should identify the affected account, likely entry method, review period, attacker activity, recipients, information involved, connected systems and known business impact. Confirmed facts should be recorded separately from assumptions and unresolved questions, and the scope should be updated as new evidence becomes available.

4. Responding to Confirmed Impact

The organization should follow every response path supported by the evidence. Several paths may operate at the same time, under the same incident leadership and communications plan.

1. **Fraudulent messages —** Trace affected messages and recipients, preserve a representative copy, remove or retract internal copies where possible, block malicious links or domains, and warn recipients through a trusted channel. Determine whether anyone replied, opened a link, supplied information or followed instructions.

2. **Payment, payroll or banking fraud —** Continue urgent coordination with financial institutions. Verify instructions independently, preserve transaction and approval records, and involve the insurer, counsel and law enforcement according to the agreed response.
3. **Information or credentials exposed —** Identify the specific information, password, token or secret involved and who received, viewed or downloaded it. Revoke links and tokens, rotate credentials or keys, remove unintended access and preserve available access records.
4. **Connected systems or administrative tools —** Identify the systems and permissions available to the affected account. Revoke sessions, rotate shared credentials, review system-side logs and confirm whether the attacker performed any actions.
5. **External recipients and third parties —** Use known contact details rather than replying to the suspicious thread. Explain what should be ignored or verified, determine whether the recipient acted, and provide one contact point for further evidence and updates.

5. Recovery and Closure

Recovery should be based on defined checks rather than a password reset alone. Access can be restored gradually while higher-risk functions remain restricted or monitored.

1. **Account verified —** The password, legitimate MFA and recovery methods, active sessions, forwarding, rules, delegates, mailbox permissions and application access have been reviewed.
2. **Device verified —** Relevant endpoints are confirmed safe, isolated for further work or rebuilt, and credentials exposed on an affected device have been rotated.
3. **Access restored —** The user signs in through a trusted route and receives only the access needed. Temporary restrictions and dependencies are recorded.
4. **Monitoring completed —** The organization sets a risk-based monitoring period and reviews sign-ins, identity changes, mailbox activity and related alerts for repeated misuse.

Closure record

- A clear timeline, affected accounts, entry method, evidence locations, confirmed impact and unresolved limitations.
- Communications issued, decisions made and legal, insurer, regulatory or law-enforcement reports completed or considered.
- Remaining corrective actions with a named owner, target date and route for tracking completion.
- A review of what helped or delayed the response and what should change before the next incident.

6. Preventing Recurrence

The post-incident review should turn confirmed findings into practical improvements. Controls should address both technical compromise and the business processes that allow a fraudulent request to succeed.

Strengthening identity

- Require phishing-resistant MFA where possible and apply conditional-access policies based on user, device, location and risk.
- Disable unnecessary legacy authentication, protect privileged accounts, and review recovery methods and application consent.

Protect email

- Implement and maintain SPF, DKIM and DMARC, and monitor forwarding, mailbox rules, delegates and suspicious sign-ins.
- Restrict automatic external forwarding where it is not required and review mailbox settings periodically for unauthorized changes.

Verify transactions

- Require independent verification for new bank details, payment changes, payroll requests and unusual purchases.
- Use a trusted phone number or established workflow rather than contact information supplied in the request and require additional approval for higher-risk transactions.

Improve detection and endpoint protection

- Keep centrally managed endpoint protection or EDR tools, agents, policies and threat intelligence current, and confirm that all supported devices remain covered and reporting.
- Retain appropriate identity, mailbox and endpoint logs; alert on high-risk sign-ins, suspicious account changes and endpoint threats; and ensure staff know how to report suspicious activity quickly.

Prepare people

- Train employees using realistic BEC scenarios, including payment changes, impersonation, unusual MFA prompts and requests to bypass normal procedures.
- Maintain a simple reporting route and exercise the response plan with the teams expected to make decisions or take action.

Prepare partners

- Maintain current contacts for legal counsel, the cyber-risk insurer, financial institutions and relevant law-enforcement authorities.
- Agree verification, escalation and notification procedures with important suppliers and customers before an incident occurs.

Secure remote access

- Use an organization-managed device and a trusted private network or mobile hotspot where possible.
- If public Wi-Fi is unavoidable, use the approved VPN or secure-access service, confirm the network name, and disable automatic connection and unnecessary file sharing.
- Never enter company credentials into an unexpected Wi-Fi prompt or use a shared computer. Delay payment approval, banking changes and administrative work until a secure connection and independent verification are available.

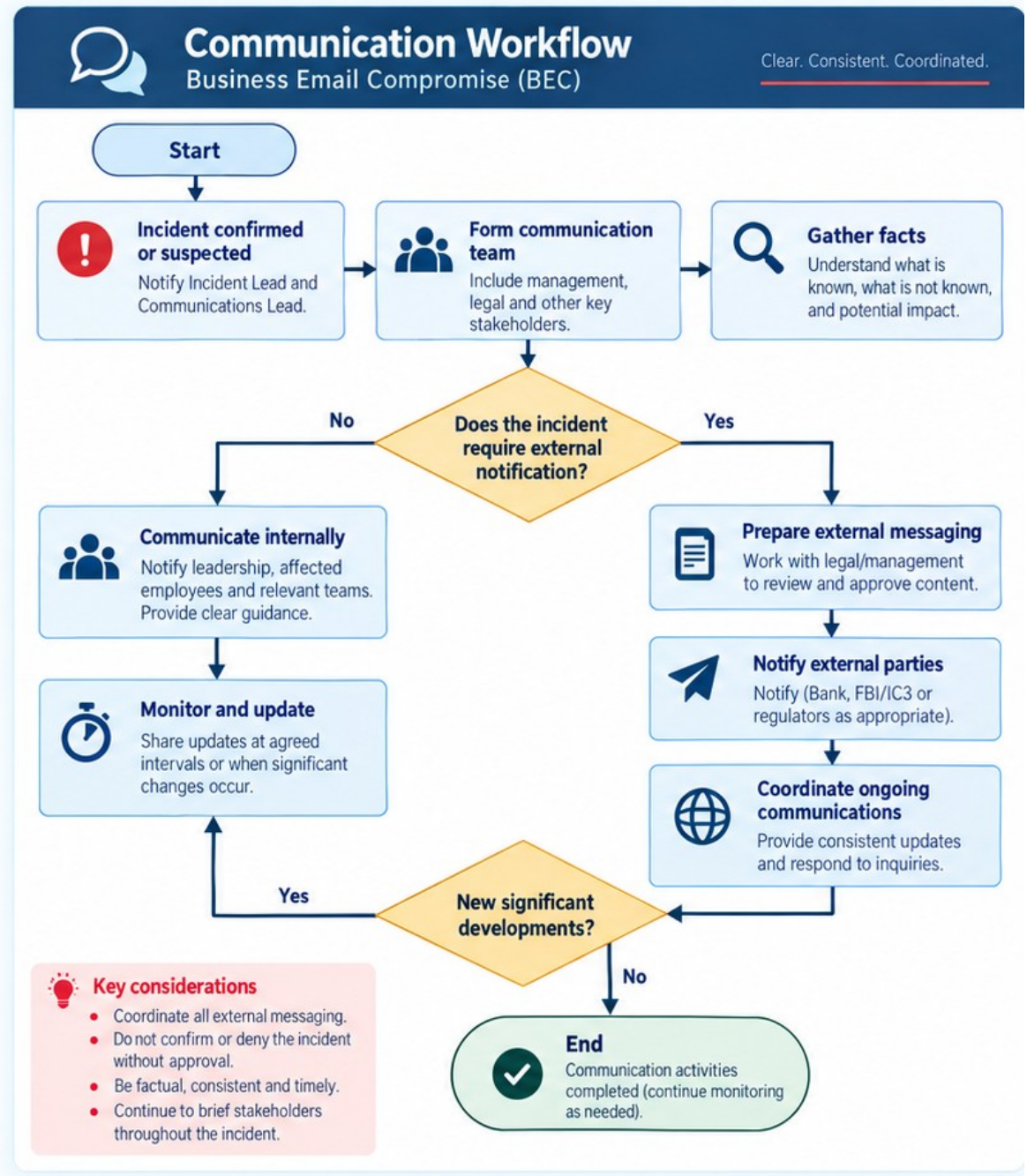
Reduce unnecessary exposure

- Review access to sensitive mailboxes, shared accounts, customer systems, files and administrative tools.
- Remove access that is no longer needed and separate high-risk duties where practical.

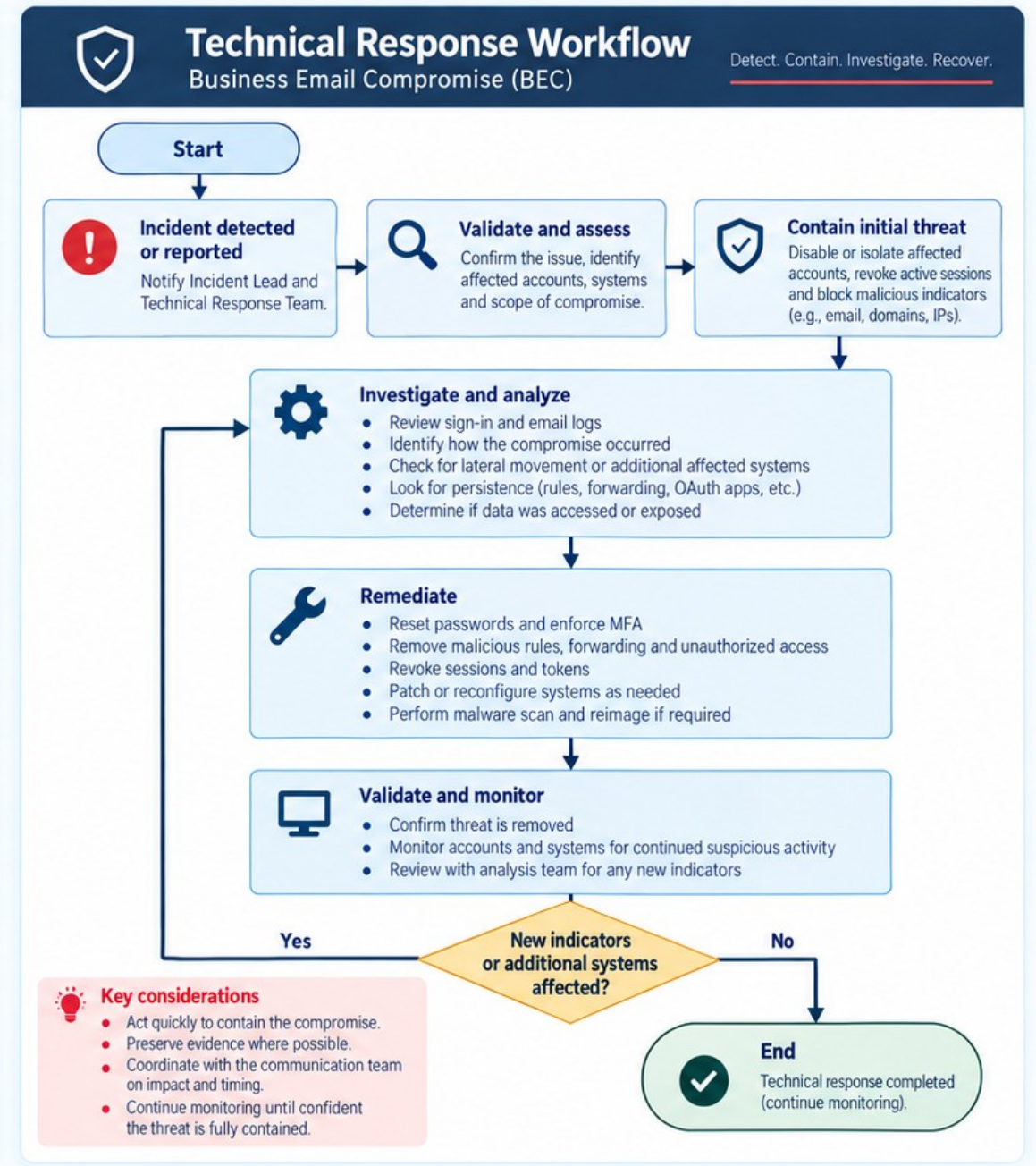
Prioritizing improvements

Correct the control weakness that enabled the incident first, but do not stop there. Priorities should reflect the organization's payment exposure, sensitive information, privileged access, important third parties and ability to detect misuse. Each improvement should have an owner, target date and evidence of completion.

Communication Workflow



Technical Response Workflow



Official resources

FBI Business Email Compromise guidance: fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise

FBI Internet Crime Complaint Center: ic3.gov

FTC Data Breach Response guide: ftc.gov/business-guidance/resources/data-breach-response-guide-business

CISA cybersecurity guidance: cisa.gov

NIST Cybersecurity Framework: nist.gov/cyberframework