The Ticking Clock

Your Comprehensive Guide to Navigating a Business Email Compromise (BEC) Crisis

LEAP STRATEGIES

Redefining Technology, Enabling Vision.

Introduction

When a crisis unfolds in the digital world, the clock is always ticking, especially when you're the target of a Business Email Compromise (BEC) attack. It's akin to a suspense thriller, where the protagonist races against time to defuse a ticking bomb. In this real-world scenario, your organisation's finances and reputation are at stake, with every minute that ticks away lessening the likelihood of recovering stolen funds.

Whether you are a CFO overseeing the financial integrity of a large conglomerate or an executive in a small-to-medium enterprise (SME), you need to have a battle plan ready. that's precisely what this guide offers: a strategic blueprint detailing how to PREPARE, PLAN, and EXECUTE a BEC incident response.

What to expect from this guide?

When in the midst of a BEC attack, time is of the essence. That is why being preemptive by creating a BEC-specific incident response plan before an attack happens is time well spent.

We understand the detrimental impact that BEC attacks can have on any business, so we have created this easy to read, step-by-step guide to help your organisation get BEC-proofed.

You can expect to learn from this guide:

- **Why a BEC-specific Plan is Crucial:** We delve into why traditional cyber-security plans don't cut it when it comes to BEC.
- **The Multi-dimensional Challenge:** Uncover why combating BEC attacks is not just an IT problem but a complex issue requiring a multi-departmental approach.
- **The Components of a Holistic BEC Incident Response:** Get actionable insights into creating a holistic plan, one that includes both preventive and reactive measures.

Contents

Why is it important to craft a BEC-specific Incident Response Plan?

During any given person's lifetime, many lessons are only learnt after making a mistake. In cyberspace, mistakes are not only costly, but can be detrimental to an organisation's continuity. These days, incident response plans are usually developed in the aftermath of a cyber attack. This reactive planning may not be enough if faced with a BEC attack.

To effectively address the complexities of a BEC attack, organisations must revise their general cyber incident response plans to incorporate controls fit-for-BEC-purpose.

Here's where a dedicated BEC incident response plan veers off the beaten path:

- Urgency Is Paramount: A BEC-specific plan emphasises the need for rapid response when engaging with an incident. It aims to engage and deliver the right information to key financial institutions swiftly, so they can halt outgoing payments.
- Targeting Internal Weak Spots: BEC attacks often exploit gaps in internal financial controls, particularly in the Accounts Payable function. A BEC-specific plan can pinpoint these vulnerabilities - whether technical or human, and offer solutions to harden them.

When it comes to BEC attacks, some unique features apply that set them apart from other types of cyber-attacks. That's why organisations should develop a dedicated BEC incident response plan.

Who's on the BEC Incident Response Team? (Hint: It's Not Just IT!)

In the aftermath of a cyberattack, the IT teams or cyber incident responders are the knights in shining armour. However, while they wield powerful swords (or keyboards), battling BEC is akin to facing a hydra: it's multi-headed, requiring an army to conquer it. It is imperative that the CFO and financial executives join forces with the IT team to provide a well-rounded defence and offence.

This multi-dimensional approach acknowledges that BEC attacks exploit technical, human and financial weak points. Therefore, an effective BEC incident response plan should be multifaceted.

Why should BEC Response be Swift and Incisive?

Let's refer to MoneySmart, an Australian financial advisory initiative. They suggest that recovering money from mistaken transactions is possible within specific time frames. But let's be honest, this isn't a lost-and-found situation; we are dealing with seasoned criminals who move fast, have nothing to lose but everything to gain. So, there are other options than waiting for ten days or more. Swift action is your only ally in disrupting the criminals' plans and possibly recovering your funds.

Crafting a Holistic BEC Incident Response Plan

A holistic approach is your Swiss Army knife in combating BEC attacks. It's comprehensive, versatile, and incredibly effective if used correctly.

- **Preparation:** This phase ensures all the required data is easily accessible for electronic discovery, aiding in legal pursuits and insurance claims.
- **Attribution:** This can help identify the perpetrators and provide valuable intelligence to law enforcement agencies.
- **Financial Tracing:** This involves working closely with financial institutions to trace and possibly reclaim stolen funds.

In essence, a holistic BEC plan is like building a fortress. While the groundwork (preparation) makes the foundation strong, it's the action plan (execution) that adds the defensive walls, the turrets, and the moats.

Part 1

Preparation

Timeline for a Holistic BEC Incident Response Plan Preparation

Being well-prepared is crucial for crafting a comprehensive BEC (Business Email Compromise) incident response strategy.

Quick access to vital data can be a game-changer between reclaiming your financial assets and suffering a loss. This indispensable information is a roadmap for banks and law enforcement to locate and retrieve stolen funds.

For this reason, CFO's must maintain a close working relationship with their IT departments to ensure they are constantly recording all relevant data needed in the aftermath of a BEC attack. Here's a detailed 3-phased breakdown of a Preparation plan.

Phase 1: Pre-Attack Planning

1. CFOs liaise with IT Teams.

Goal: Ensure essential logs are in place and accessible.

Critical Discussion Points: Financial and logistical considerations for log storage, purpose of evidence (legal or internal use), and how to ensure integrity in data collection

Phase 2: Logging Implementation

1. Event Logging

Goal: Implement comprehensive logging across all systems.

Critical Discussion Points: Availability of logs to third-party incident responders and credential sharing.

2. Email Forwarding Logging

Goal: Establish and monitor rules for email forwarding.

Critical Discussion Points: Review authorisation mechanisms, and maintain an approved list of forwarding rules.

3. Login Logging

Goal: Record details of all login activities.

Critical Discussion Points: Unusual IP addresses, logins outside business hours, and failed login attempts.

4. Privilege Escalation Logging

Goal: Keep records of all privilege escalations.

Critical Discussion Points: An updated list of accounting function users and their required privileges.

5. API and OAuth2 Logging

Goal: Monitor application interfaces and authentication tokens.

Critical Discussion Points: Communication lines between IT and accounting/finance teams in case of breaches.

6. Data Exfiltration Logging

Goal: Detect unauthorised data transfers.

Critical Discussion Points: Immediate communication lines to accounting and finance teams to rapidly identify BEC instances.

Timeline for a Holistic BEC Incident Response Plan Preparation

Phase 3: Forensic Readiness

1. Log Retention Strategy

Goal: Store logs for a sufficient period.

Critical Discussion Points: Balancing the cost and risk.

2. Evidence Integrity

Goal: Ensure the integrity of log data.

Critical Discussion Points: Courts of law may use data as evidence.

Data Points	Description	Importance	Key Information	Discussion Points with IT Team
Event Logging	Logs and records system events, including user access and activity.	Establish a chain of events leading up to a BEC attack.	- Unified Audit Log (UAL) Administrator Audit Logs (AAL) Message Trace Logs (MTL)	Immediate accessibility of logs, availability of credentials.
Email Forwarding	Rules in email systems for automatic forwarding.	Identify automated rules set up by scammers for reconnaissance and data collection.	Emails being forwarded to external mailboxes, specific keyword-based rules.	Disable unauthorised rule creation, maintain an approved list of rules.
Login Logging	Records of login attempts.	Track unauthorised or suspicious login activities.	IP and MAC addresses used for login.	Record all logs in the Unified Audit Log (UAL), alert systems for log tampering.
Privilege Escalation	Records of privilege changes in user accounts.	Track changes that give higher-level system access to users.	Permission changes in individual mailboxes, folder-level permissions.	Maintain a current list of users and their required privileges.
API & OAuth2	Logs related to application interfaces and authentication tokens.	Monitor vulnerabilities and authentication bypass attempts.	Usage and breach instances.	Breach communication between IT and accounting/ finance teams.
Data Exfiltration	Logs indicating unauthorised data transfers.	Detects multiple attack vectors that may be leveraged along with BEC.	Session IDs, IP/MAC addresses, data destinations, methods used.	Immediate communication lines to accounting and finance teams.

Part 2

Planning

Critical Components of a BEC Incident Response Plan

After establishing a meticulous record of all the essential data, it's time to start planning a BEC incident response. This plan should be ready for immediate deployment when a BEC attack is detected.

Your BEC incident response blueprint should encompass several vital components:

- Explicit objectives and prioritised goals
- A designated BEC incident response team, complete with a transparent chain of command and responsibilities
- A well-defined procedure to follow in case of an incident

Setting Clear Objectives and Priorities

Upon the detection of a BEC attack, quick and calculated decision-making is indispensable. Your plan should start by delineating explicit objectives and pinpointing what will take precedence.

The foremost objective will be to reclaim any misappropriated funds.

Secondary objectives might include:

- Determining who orchestrated the attack
- Uncovering clues that could lead to the stolen money's destination
- Identifying any internal participants involved
- Identifying potential exploits by assessing internal controls for vulnerabilities.

Remember that you can continually update and modify your BEC incident response plan as needed. Periodic workshops and consultations involving senior figures from the finance, IT, and cybersecurity departments will enable you to refine your preparedness continually and foster your cybersecurity posture. These sessions can include training simulations and updating measures to bolster your resilience and cyber maturity.

Establishing an Incident Response Team

As you develop your BEC incident response protocol, carefully contemplate the composition of your incident response squad.

The team will take on responsibilities such as

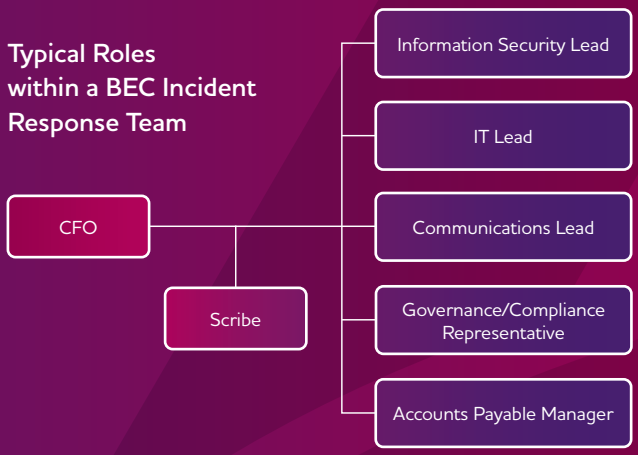
- Monitoring inspecting and analysing incident-related data
- Orchestrating activities surrounding the incident
- Relaying crucial messages to internal and external stakeholders

Team members should be actively engaged in creating the response plans, as this ensures everyone is on the same page regarding their roles.

The response initiative should ideally be headed by the CFO, given the financial ramifications of BEC attacks. However, IT and cybersecurity specialists will also serve pivotal functions.

The team may need to broaden its composition depending on the specific nature of the BEC attack. What's crucial is that the team members possess both the expertise to evaluate the incident's scope and impact, as well as the authority to take swift action.

Typical Roles within a BEC Incident Response Team



Role	Responsibilities
CFO	Central authority in charge of coordinating response activities. Manages communication with financial institutions for fund tracking, halting, and retrieval. Oversees interaction with law enforcement.
Scribe	Supports the CFO by chronicling all activities and organising timelines for each phase of the response.
Information Security Lead	Examines log data to piece together the attack's origin and other attributes that can aid the investigation.
IT Lead	Supplies investigators with necessary logs, and imposes lockdowns on systems, like email clients, when needed.
Communications Lead	Handles internal and external communications with concerned parties.
Governance/Compliance	Provides legal counsel on issues ranging from data breaches to insurance and legal claims.
Accounts Payable Manager	Investigates any lapses in internal financial controls exploited during the attack and identifies areas for improvement.

The BEC Incident Response Workflow

The specifics of your incident response may differ based on the unique context of a BEC (Business Email Compromise) attack. However, a structured process divided into priority zones can serve as a general framework to guide your actions. Here's a staged approach:

RED ZONE: Immediate Action
Breach Discovery: Detecting the cyber incident is the first critical step.
Engage IT & Cybersecurity: Immediately alert the IT and cybersecurity units for an immediate assessment.
Secure Email Systems: Swiftly lockdown email systems to prevent further unauthorised activities.
Reach Out to Financial Bodies: Inform financial institutions to be on the lookout for unusual activities.
Contact Law Enforcement: Initiate a conversation with appropriate law enforcement agencies for legal proceedings.

The BEC Incident Response Workflow

ORANGE ZONE: Secondary Measures

Data Analysis: Review relevant data logs and system analytics to grasp the breach's magnitude and origins.

Evidence-Based Investigation: Use all accessible evidence, such as system logs, email trails, and firsthand accounts, to document the breach's events.

Maintain Communication: Regularly sync with banks and law enforcement to stay updated on financial recoveries or legal developments.

YELLOW ZONE: Tertiary Steps

Inform Stakeholders: It's vital to keep all relevant parties, including regulators, shareholders, employees, and potentially impacted suppliers in the loop.

Assess & Strengthen Internal Controls: After managing the immediate threats, focus on diagnosing and strengthening the weak spots in your Accounts Payable and overall cyber infrastructure.

Part 3

Execution

Execution of BEC Incident Response Plan

Responding promptly to a Business Email Compromise (BEC) attack can distinguish between recovery and significant financial loss. Below is a structured checklist to tackle each crucial aspect without delay.

1st Priority

Step 1: Activate IT & Cybersecurity Protocols

Immediately after suspecting a BEC attack, alert your IT system administrators and cyber security leads. These leads could be from within your organisation or external specialised responders.

There's a good chance your IT administrators will have to temporarily restrict access to various systems and devices to hinder further attacks and thoroughly investigate the extent of the breach.

Step 2: Engage with Financial Institutions

Speed is of the essence. Aim to halt any unauthorised transactions as soon as possible. Once the compromised funds reach the beneficiary's bank, the scammer will rapidly:

1. Empty out your funds.
2. Move your funds to third-party accounts, often abroad.
3. Convert your funds into less traceable forms, like cryptocurrencies.

A delay in reporting the attack to your bank drastically diminishes your recovery odds. Hence, maintain a list of senior personnel with emergency contacts of bank representatives. This ensures immediate action at any hour. Remember, all major Australian banks possess dedicated teams to assist clients affected by scams. It's paramount to have these contacts on hand.

Execution of BEC Incident Response Plan

Step 3: Contact Law Enforcement

Though the chances of recovering stolen funds are slim, it's crucial to report the BEC attack to your local police, who can involve federal agencies like the Australian Federal Police (AFP). The AFP collaborates with international law enforcement bodies to track BEC heists.

Additionally, notify governmental bodies such as:

- The Australian Cyber Security Centre (ACSC): They can alert the AFP, aiming to halt fund transfers.
- Scamwatch: This service, provided through the Australian Competition and Consumer Commission, offers guidance tailored to your situation.

Step 4: Secure Email Systems

The modus operandi of BEC attacks varies attackers might have:

- Penetrated your email via phishing, social engineering, or malware.
- Breached your supplier's email system.
- Used tactics like email spoofing.

Since the exact method might remain elusive initially, it's imperative to secure all organisational email systems. Moreover, establish a non-email communication strategy to engage with essential parties like staff, clients, suppliers, etc. Consider maintaining a phone database or leveraging instant messaging platforms for urgent communication in the event of an incident.

Prolonged email system downtime might ensue, depending on the investigation's duration. Constant communication reassures stakeholders, helping to manage reputation risks.

In a BEC scenario, swift, organised, decisive action can often lead to damage control. This step-by-step execution ensures you don't overlook any pivotal areas during the high-pressure moments following the detection of a cyber-incident.

Execution of BEC Incident Response Plan

2nd Priority

Step 5: Preparation Through Data Logging

Before falling prey to a BEC attack, it's paramount to be proactive. Make certain your organisation is actively logging crucial data that would be instrumental for a subsequent investigation. It's the duty of the IT team to extract this valuable data from logs and present it to the investigators. This promptness ensures that the experts can quickly delve into assembling evidence, which is pivotal for any endeavour to reclaim misappropriated funds.

Step 6: Comprehensive Evidence-based Investigation

The nature of BEC attacks is intricate, likened to solving a multi-dimensional puzzle. A deep dive into the available logs and data is imperative to reconstruct the sequence of events. While your in-house IT and cybersecurity teams are adept, BEC-specific inquiries might necessitate specialised skills. There's a probability that you'll need to enlist the services of seasoned incident response professionals. These experts, adept in swiftly pinpointing the breach source, attributing blame, and tracing your funds, can be game-changers.

This optimises transmitting pivotal information to banks and law enforcement, bolstering the likelihood of catching the culprits and recuperating your assets.

Step 7: Sustained Coordination with Financial and Legal Entities

Once your evidence trove is ready, time is of the essence. Promptly share all pertinent information derived from your data with both your bank and the legal authorities. This aids their independent investigations and augments the possibility of a favourable resolution.

3rd Priority

Step 8: Communication with Other Stakeholders

In the aftermath of a BEC attack, envision a ripple effect in a pond. The impact and the need for information dissemination might span to a broad spectrum of stakeholders. Firstly, liaise with suppliers, especially if they were supposed to be the beneficiaries of the payments.

Peeling back another layer reveals a broader gamut of entities, contingent on the specifics of the BEC episode. Was other data compromised? If so, you may need to notify the relevant regulators, shareholders, and the affected customer base. In an age where information travels at the speed of light, brace yourself for potential media probes. Here's where the adage "Honesty is the best policy" shines. Transparent crisis communication is akin to using an umbrella during a storm; it won't stop the rain, but it offers protection. It goes a long way in curbing the possible onslaught on your reputation.

Step 9: Audit and Fortify Vulnerabilities in AP

A BEC attack is insidious, exploiting not just some technical chinks but finding vulnerabilities in the Accounts Payable (AP) function's internal controls.

Now, think of this as a detective revisiting a crime scene. A meticulous sweep, or in corporate terms, an exhaustive audit of AP protocols, is mandatory. This deep dive will unmask how the adversary outmanoeuvred your checks and balances. Were there Trojan Horses internally? Equipped with these insights, chart out a strategy to plug these loopholes.

Conclusion

BEC attacks are a formidable challenge in the cyber realm, with their intricate blend of exploitable technical oversights and internal process vulnerabilities. Their adaptability and evolving sophistication often result in funds being syphoned off to offshore accounts or metamorphosing into elusive cryptocurrencies.

In this treacherous digital landscape, the axiom "prevention is better than cure" has never been more pertinent. While having an astute BEC incident response strategy is imperative, it's often the preventative measures that become the cornerstone to safeguarding assets.

With this knowledge in your arsenal, it's pivotal to align with a trusted partner who understands the intricacies and nuances of these cyber threats. LEAP Strategies stands ready as your compass and is here to shield you in this endeavour.

As a beacon in the cybersecurity space, we not only guide you through the meticulous process of drafting and enacting a robust BEC defensive strategy but also offer unwavering support should you face the unfortunate event of an attack. Reach out to LEAP Strategies today and fortify your organisation's bulwarks against the lurking cyber adversaries.

LEAP
STRATEGIES
Redefining Technology, Enabling Vision.

Find out how LEAP Strategies can help secure your payment system.

www.leapstrategies.com.au