The Most Lucrative
Form of Cybercrime

A CyberLeader
White Paper on

Business Email Compromise

advance

INTRODUCTION

In their 2020 review of activity, the ACCC reported that Business Email Compromise (BEC) had become the leading cause of financial loss to scams in Australia, costing a total of $132 million[1].

Given the growing frequency and cost of these attacks, Business Email Compromise represents a very real risk to both Australian and international businesses.

Unfortunately, due to its emerging nature, many organisations do not fully understand the risk and do not have adequate protections in place to mitigate it.
This paper will explain the methods of BEC attacks, and the potential actions organisations can take to protect themselves.

Business Email Compromise is an attack-type that is characterised by the attacker impersonating an identity known to the target. Once the attacker has successfully impersonated an individual, the attacker then leverages the relationships the individual holds to subvert funds, goods or sensitive information.

BEC is a form of social engineering, which limits the effectiveness of technology solutions as a defence, as BEC emails do not contain malware or malicious links. As a result, increased emphasis is needed on the people and process elements of an organisation's defensive layers.

BEC attacks vary greatly in the amount of research and effort on the part of the attacker. While some attackers may opt for the high volume low effort approach, others may spend many hours reviewing corporate and personal publications and social media to gain an understanding of internal relationships, hierarchy, branding, processes and controls to tailor their attack.

Given the average successful BEC attack results in losses of $157,000 USD[2], it is not hard for a sophisticated attacker to justify lengthy, in-depth research of a target.

By combining in-depth research about the individual and the organisation, exploiting existing trusted relationships and incorporating traditional social engineering techniques such as urgency and emotional engagement, attackers can form convincing situations for employees to comply with their malicious requests.

However, gaining an understanding of the methods attackers use, and taking a few simple defensive steps can result in a much better level of organisational resilience against Business Email Compromise attacks.

[1] https://www.accc.gov.au/system/files/1657RPT_Targeting%20scams%202019_FA.pdf
[2] https://www.ic3.gov/Media/Y2019/PSA190910

IMPERSONATION

There are four common methods attackers use to impersonate trusted contacts:

1. The email 'sender' attribute is changed through a variety of methods.

2. Real first and last names of the impersonation victim are used to register a free email address (such as Hotmail or Gmail).

3. A fake domain is registered that looks visually similar to the real domain (@Mircosoft.com instead of the @Microsoft.com, or replacing the letter L with the number 1).

4. Legitimate credentials are stolen by the attacker through phishing or data breach.

Common types of Business Email Compromise attacks:

1. **CEO Impersonation** – due to their authority, CEO's and other senior staff members are often the targets of impersonation. The attacker will then masquerade as the authority figure and request payments be made, or sensitive data sent to external locations.

2. **Supplier Impersonation** – in business-to-business relationships, large financial sums are routinely transferred. If an attacker can successfully impersonate a supplier, they will attempt to have banking details 'updated' so the next legitimate payment is diverted to the attacker's bank account.

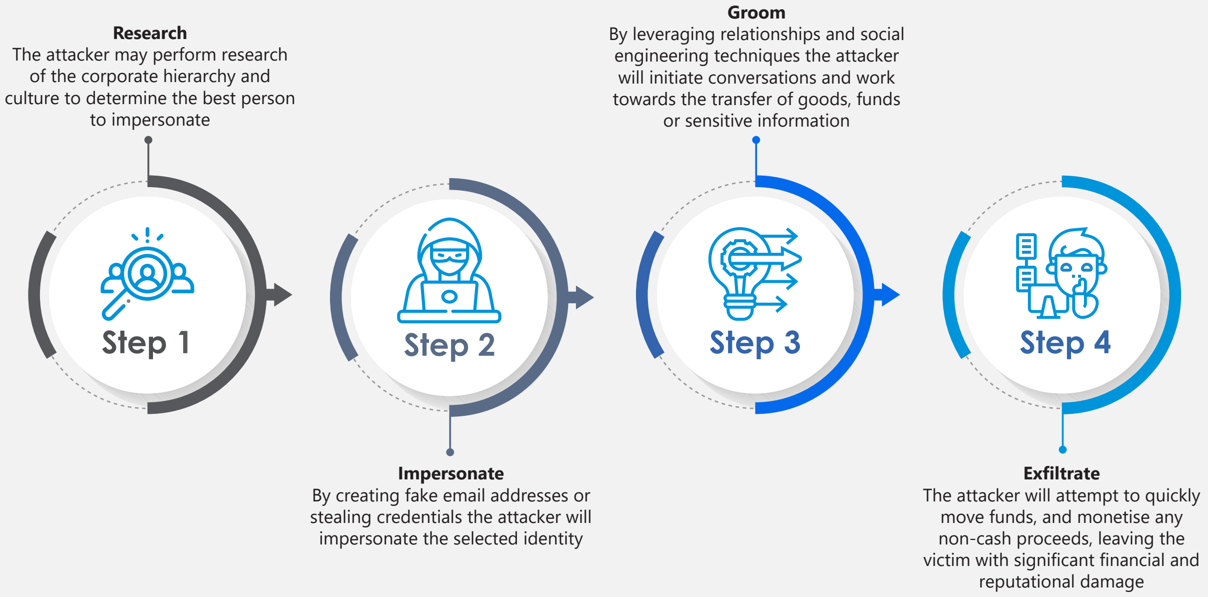
Note: This is also common outside of the business world, with attackers targeting tradespeople, and producing fake invoices to trick individuals into paying large sums into the wrong bank accounts.

3. **Employee Impersonation** – A common attack vector as it can be carried out from almost any corporate email account, Employee Impersonation sees the attacker attempt to have a legitimate employee's bank account details 'updated' so their next salary payment is diverted to the attacker's bank account.

4. **Customer Impersonation** – By impersonating a customer in a business-to-business relationship an attacker will fake purchase orders and attempt to have goods delivered to the attacker for resale.

5. **Gift Card Fraud** – With increasing regularity attackers will use gift cards to extract value from an organisation. Once impersonation has been achieved the attacker will request the victim purchase them gift cards and email the serial numbers, often with the promise of remuneration through expenses. The gift card serial numbers are then resold on the black market.

Four Steps of Business Email Compromise



Research
The attacker may perform research of the corporate hierarchy and culture to determine the best person to impersonate

Impersonate
By creating fake email addresses or stealing credentials the attacker will impersonate the selected identity

Groom
By leveraging relationships and social engineering techniques the attacker will initiate conversations and work towards the transfer of goods, funds or sensitive information

Exfiltrate
The attacker will attempt to quickly move funds, and monetise any non-cash proceeds, leaving the victim with significant financial and reputational damage

Defending Against BEC Attacks

Board Discussion – An important first step is to ensure the risk of BEC, and social engineering in general, is understood and discussed at the board level.
BEC is not solely an IT issue, with Finance and Payroll departments disproportionately represented amongst BEC targets. To effectively mitigate BEC a unified approach is required across departments to ensure a high level of organisational resiliency.

Training and Awareness – As with many forms of social engineering, training and awareness are very effective defences. Individuals who are alert to the possibility of email compromise and impersonation are much less likely to fall victim to Business Email Compromise.

Simulations – To further build upon training, and ensure knowledge retention, simulated BEC attempts should be run regularly. Simulations have the added benefit of providing hard metrics to help quantify the size of the issue, and accurately measuring the progress of improvements.

Identify 'at Risk' Roles – depending on the organisation, there may be some roles at more risk of BEC than others. Examples may include Finance staff, Payroll staff, Executive Assistants and Service Desk staff (for credential resets). Once these roles have been identified they can be provided enhanced training or more frequent simulations to improve the organisations overall resiliency and improve the ROI of investment made to mitigate BEC.

Email Gateway Tagging – Modern email gateways can be configured to tag emails from external sources and add BEC or phishing warnings. This helps prevent certain types of impersonation tactics and keeps the possibility of BEC front of mind for staff dealing with external emails.

Anti-Spoofing - To protect your business partners and your business reputation, anti-spoofing configurations such as SPF, DKIM and DMARC can be implemented to prevent your domain from being spoofed in a BEC attack against suppliers or customers.

DLP – DLP, or Data Loss Prevention refers to a set of tools and processes designed to reduce the risk of sensitive information leaving the corporate environment. These can be very effective at preventing email compromise attacks that target sensitive information.

Domain Awareness – To prevent impersonation by small changes being made to an organisation's domain, many organisations will register similar domains to prevent attackers from using them. Alternatively, where registration is not possible or feasible, visually similar domain names can be pre-emptively blocked or flagged at the email gateway.

Robust Business Processes – BEC ultimately relies upon impersonation. Business processes should be designed with this in mind, and include identity validation steps utilising known contact methods, such as voice calls using numbers stored in the corporate directory.

Least Privileged Access – Least Privileged Access is a common concept in IT Security, ensuring individuals are provided with the minimum possible access required to complete their roles. This concept is not always unilaterally accepted in wider business areas, resulting in staff having access to update banking information or make financial transfers when it is not strictly required for their role. By applying the least privileged principles across other departments the risk of BEC can be greatly reduced.

B2B Transparency – When selecting vendors or even customers, organisations can incorporate an open and transparent discussion about security practices to ensure security throughout the supply chain.

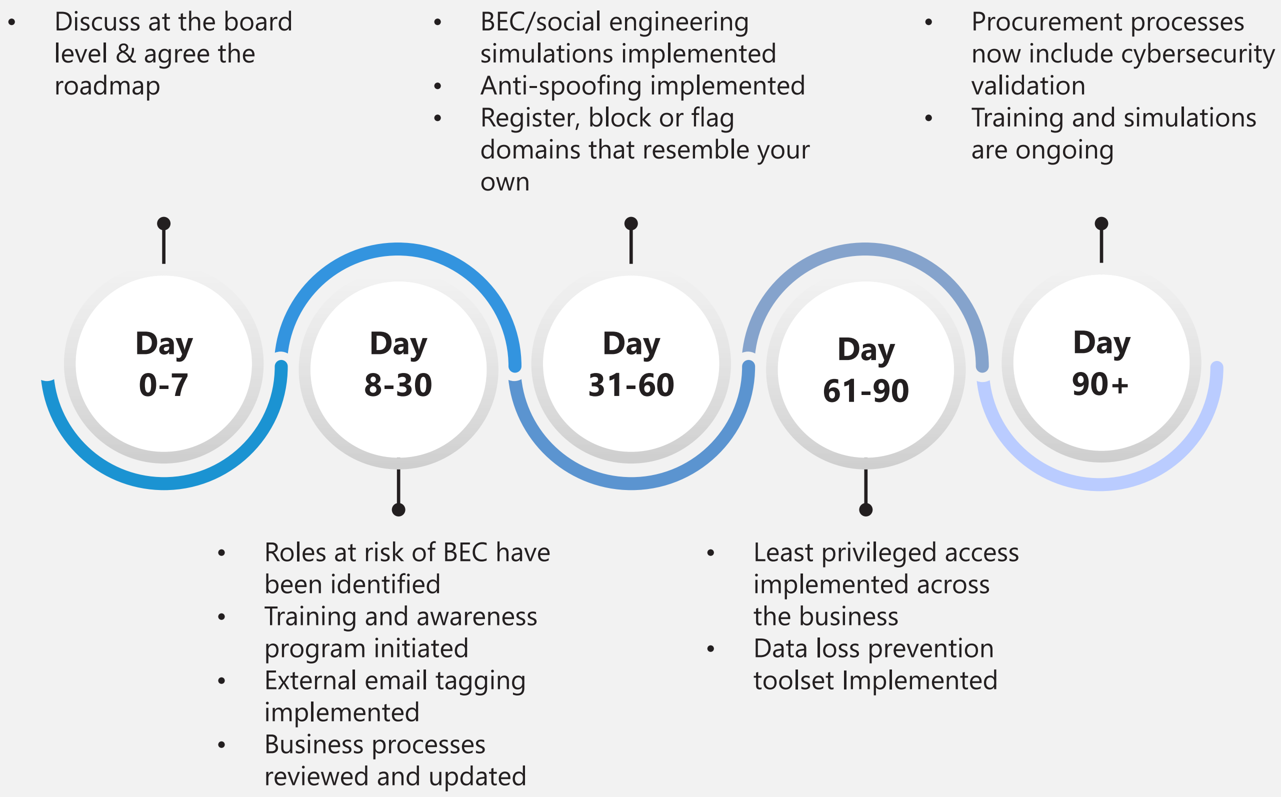
Conclusion

As the pace of business becomes faster and faster cybercriminals are using this to their advantage, exploiting busy and untrained employees. Using a variety of impersonation methods and a wider still variety of attack vectors cybercriminals are increasingly able to mimic legitimate communication and successfully subvert funds, goods and sensitive information.
The success of the practice has resulted in a sharp increase in attacks, and many organisations are not fully prepared to resist them.

To meet this growing threat the IT department cannot work in isolation, as resiliency is best achieved through an aware and vigilant user base, supported by strong business processes and underpinned by technology solutions configured to meet the organisation’s specific requirements.
Fortunately, even as this threat becomes more prevalent in the coming years, achieving these layers of defence does not require significant investment from the organisation, and small actions can provide a great return on investment when mitigating the risk of Business Email Compromise.

To help our partners protect themselves from Business Email Compromise we have included a templated roadmap to implement the protections noted on previous pages.

Template Roadmap to Address Business Email Compromise



Day 0-7

- Discuss at the board level & agree the roadmap

Day 8-30

- Roles at risk of BEC have been identified
- Training and awareness program initiated
- External email tagging implemented
- Business processes reviewed and updated

Day 31-60

- BEC/social engineering simulations implemented
- Anti-spoofing implemented
- Register, block or flag domains that resemble your own

Day 61-90

- Least privileged access implemented across the business
- Data loss prevention toolset Implemented

Day 90+

- Procurement processes now include cybersecurity validation
- Training and simulations are ongoing

Contact Info

● +61 8 8238 6500

● sales@advance.net.au

● https://www.advance.net.au/

advance