Deloitte.

Cybercrime in Tasmania
Cyber Fraud and Business Email Compromise (BEC)

November 2016

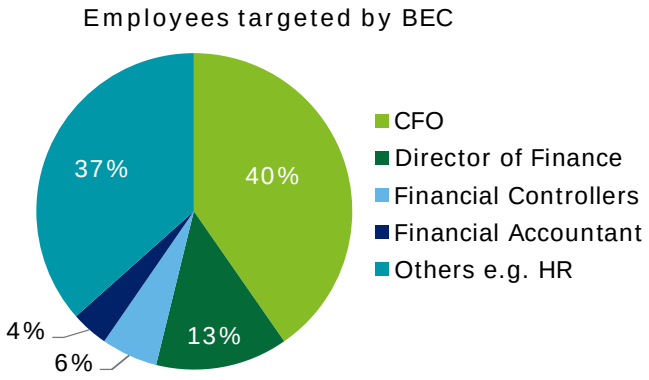
Cybercrime in Tasmania

Cybercrime is on the increase and Tasmania is not immune. A recent Tasmania Police media release[1] has identified the prevalence of sophisticated cyber criminals targeting individuals and organisations across the state. Cyber criminals are using sophisticated methods of online social engineering, including stylised and targeted phishing emails, commonly known as Business Email Compromise (BEC), to de-fraud organisations across Tasmania. In one recent example an organisation suffered a loss in-excess of $200,000 from a single incident.

What is BEC?

BEC occurs when attackers use compromised or fraudulent email addresses to target specific employees within organisations requesting a 'legitimate' transaction to be processed or changes to be made in key payment/supplier information. These sophisticated emails either appear to be from a senior member of the organisation to gain access to or make a request for funds or changes in payment details.

Trend Micro, 2016[2]



How prevalent is BEC?

A report[3] by the Federal Bureau of Investigation highlighted that in the last two years over US $3.1 billion was lost to BEC crimes. The Australian Competition and Consumer Commission's Targeting Scam Report[4] states that in 2015 AU $84.9 million was lost to scams in Australia and over 100,000 reports of scams were made. In Tasmania alone, Tasmania Police reported fraud offences have increased by 26.4% since 2013 with cyber fraud constituting 25.4% of all fraud offences in Tasmania in 2015-2016[5].

How does BEC occur?

Cyber criminals are using publicly available information from organisation websites, directories, databases and social media platforms to target specific employees within organisational areas such as finance, human resources and senior management. Below are five types of BEC that can occur in your organisation:

Changed supplier details	A fraudulent email sent to your organisation's customer base to advise of new payment information or methods of payment for invoices from your organisation.
Email replication	Hacked or replicated email domains of managers and directors are used to send out requests to the finance team to make an urgent payment.
Foreign suppliers	A fraudulent email requesting staff to transfer funds in regards to a fictitious invoice or transaction. This can be done by hacking, social engineering or by utilising similar domain names.
Executive/attorney impersonation	Impersonation of lawyers or representatives of law firms claiming carriage of urgent and confidential matters and requesting immediate transfers of funds.
Data theft	Targeting human resourcing or accounting departments to fraudulently request employee records using a compromised email. This information can then used for further BEC scams or identity fraud.

[1] http://www.police.tas.gov.au/news-events/media-releases/cybercrime-offences/
[2] http://www.trendmicro.com.au/vinfo/au/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise
[3] https://www.ic3.gov/media/2016/160614.aspx
[4] https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2015
[5] http://www.police.tas.gov.au/about-us/corporate-documents/crime-statistics-supplement/

Case Studies

Fraudulent request for payment - March 2016

The Finance Officer of a nation-wide company based in Hobart received an email from their CEO asking them to prepare an electronic transfer of funds to the value of $35,000. The email appeared to have been sent from the CEO's iPad. The payment was for a normal service of the company and to a NSW Westpac account. A number of emails were exchanged between the Finance Officer and the CEO regarding the payment. The Finance Officer prepared the payment and just prior to transferring the funds, the CEO happened to walk past the Finance Officer's desk. The Finance Officer informed the CEO they were just about to send the funds which the CEO indicated they knew nothing about it. The payment was stopped as a result. The email address of the CEO had one letter changed. The IP address of the origin of the email appeared to be out of Europe. The company put internal processes in place to prevent any future attempt and police are investigating.

Fraudulent request for payment update - May 2016

Another email was received by the Finance Officer from the CEO this time for $44,000. The email contained the same communication except on this occasion the 'sender' stated they were busy and not to contact them about this matter and to ensure it was sent immediately. On this occasion, the internal processes detected the issue and no funds were paid. The nominated account belonged to an Australian in Victoria.

Changed supplier details - July 2016

A Tasmanian company received an email from a client querying an email they received from the owner about directing future payments to a new bank account. The owner stated to the caller that there had been no change in the bank details. The email appeared to come from the owner of the company and all details were correct as the cyber criminal had hacked the owner's device sending the emails on their behalf, deleting the emails after they were sent. The owner contacted police and he was advised to communicate with all his clients to warn them of a suspected breach of his email system. Three clients have indicated that they made payments as per the email. The clients paid $3000, $1980 and $12,000 respectively to three different accounts. The accounts belonged to Australian residents. The funds have now been sent overseas and are unrecoverable. The company's email system was compromised through poor password protection. Once into their system the cyber criminals could view all emails and gather sufficient information to then contact the clients.

How can you identify and avoid BEC?

In order to avoid becoming a victim of a BEC scam, individuals should take the following precautions when actioning emails:

Independently verify – Contact the person making the request via phone or in person to confirm the request.

Content – Does it ask you to click on an unfamiliar link or download an attachment? Does the email contain errors, or is it illogical or unusual in its language or request?

Hyperlinks – If you hover the mouse over a hyperlink, does the content match the actual link?

Attachments – Is the title or format unfamiliar or different from the request? The only file types that are always safe are .txt files.

Address – Does it match the business name, are there discrepancies in the spelling or order of the name if internal, or is it from an outside source that is suspicious?

Subject – Is the subject irrelevant or different from the content of the letter? It may state that it is a reply to an email you have not sent.

How can you reduce the risk of compromise to your organisation?

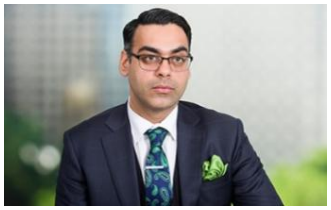
Reducing the risk of BEC compromise requires technical, procedural and educational controls in order to be secure, vigilant and resilient:

- Raise employee awareness by implementing security training and organisation-wide anti-phishing training.
- Maintain a risk-based business-aligned strategy by strengthening processes around financial transactions and third party management.
- Upgrade your secure email gateway (SEG) and ensure the most effective security controls are enabled to prevent phishing emails reaching employee inboxes.
- Deploy URL filtering, attachment sandboxing and content disarm and reconstruction (CDR).
- Ensure endpoint security and web gateway security is in place.

Contacts

Elizabeth Lovett
Partner
Risk Advisory TAS
Tel: +61 417 278 043
ellovett@deloitte.com.au

Blair Browning
Director
Risk Advisory TAS
Tel: +61 3 6237 7603
blbrowning@deloitte.com.au



Puneet Kukreja
Partner
Cyber Risk Services VIC
Tel: +61 403 037 010
pkukreja@deloitte.com.au

David Hawks
Director
Cyber Risk Services NSW
Tel: +61 2 9322 7000
dhawks@deloitte.com.au