BUSINESS EMAIL COMPROMISE

BEC – The Costs to a Business

ACP
AUSTBROKERS CYBER PRO

Business Email Compromises ('BEC') events continue to be some of the most common cyber incidents, especially for SME businesses. These incidents can cause organisations significant losses, including those associated with investigating the incident to ensure that an organisation discharges its obligations under the Privacy Act 1988 (via the Notifiable Data Breaches scheme). This paper will explore what a BEC incident is and provide a detailed analysis of *real-life* claims in this space, including the associated costs and how they can be covered off under a cyber insurance policy.

What is a Business Email Compromise ('BEC')?

A Business Email Compromise ('BEC') means unauthorised access to an employee's email inbox by a third party as a direct result of that same employee falling victim of a phishing attack that subsequently results in the use of that email account for malicious purposes.

In many cases the threat actor will attempt to use their access in the email inbox to impersonate trusted sources and convince individuals to transfer monies to fraudulent bank accounts. Whilst these transfers of funds are still occurring, we are seeing organisations becoming much more stringent with their *funds transfer* controls, which in many cases, stops these attempts in their tracks.

Despite the above, the Notifiable Data Breaches scheme under the Privacy Act 1988 requires such intrusions to be investigated to confirm whether an *eligible data breach* has occurred, i.e., is the data breach likely to cause serious harm to an individual whose personal information was compromised. If, after an investigation, the answer is yes than the organisation must notify the affected individuals and the Office of the Australian Information Commissioner ('OAIC').

The following examples are *real-life* claims where no fund transfers have occurred, however significant costs have still been incurred in the investigation of the BEC incident.

Example 1 – Manufacturing Organisation

A manufacturing organisation suffered a BEC incident which led to the email inbox of one employee being compromised. The organisation was alerted when a suspicious request for a money transfer was sent to the accounts department. No money was transferred. The costs associated with this incident are outlined below.

Incident Responses Expenses - $10,000. These costs include initial triage call, engagement of vendors to assist the Insured, ongoing discussions with the Insured to obtain information required to assist in the investigation, ongoing correspondence, reporting and updates to the insurer, review of forensic IT findings etc.

Forensic IT Costs - $7,500. These costs include complete forensic review of the affected mailbox, reviewing the methods of unauthorised access, reviewing any forwarding rules and evidence of synchronisation, including data exfiltration, and providing a detailed report of the overall findings.

Privacy Advice - $5,000. These costs include a detailed serious harm test in conjunction with any personal information that was found to be compromised in the incident, along with privacy advice in relation to whether an eligible data breach has occurred and whether notification of such incident is required under the Privacy Act 1988.

Conclusion

This incident did not require notification as it was deemed after investigation that an eligible data breach had not occurred. The total costs of this investigation were $22,500. These costs were covered under the Privacy Notification & Crisis Management Expenses section of the cyber insurance policy.

Example 2 – Accounting Organisation

An accounting organisation suffered a BEC incident which led to the email inbox of two employees being compromised. The organisation was alerted when clients began contacting them about suspicious spam emails being sent from their email addresses. The Insured was concerned given the sensitive information they hold on clients, including Tax File Numbers ('TFNs') etc. The costs associated with this incident are outlined below.

Incident Responses Expenses - $10,000. These costs include initial triage call, engagement of vendors to assist the Insured, ongoing discussions with the Insured to obtain information required to assist in the investigation, ongoing correspondence, reporting and updates to the insurer, review of forensic IT findings etc.

Forensic IT Costs - $10,500. These costs include complete forensic review of the affected mailboxes, reviewing the methods of unauthorised access, reviewing any forwarding rules and evidence of synchronisation, including data exfiltration, and providing a detailed report of the overall findings.

Further Forensic & Mailbox Assessments - $15,000. Given the information found in the affected mailboxes was concerning, further review was required to catalogue the information and break down the records and individuals connected to those records. The information at risk included TFNs and financial information of individuals.

Privacy Assessment & Advice - $10,000. These costs include a detailed serious harm test in conjunction with the TFN and financial information that was found. It was confirmed after such analysis an eligible data breach had occurred and notification to individuals and the OAIC was required.

Notification Campaign Costs - $15,000. These costs relate to notification costs, which include, drafting notification letters to individuals and regulators, liaising with the Australian Tax Office ('ATO') and the OAIC, communicating with stakeholders within the organisation and fielding queries from individuals and regulators in relation to the notifications.

Conclusion

This incident did require notification as it was deemed after investigation that an eligible data breach had occurred. The total costs of this investigation were $60,500. When an eligible data breach occurs and review and notification is required under the Privacy Act 1988, the costs in relation to the BEC incident can be significantly higher than when notification is not required. These costs were covered under the Privacy Notification & Crisis Management Expenses section of the cyber insurance policy.