Borderless CS
CYBER SAFE TOGETHER

Digital / Email Forensic
Customer success story

CLIENT: **PROSPER LAW PTY LTD**

INDUSTRY: **LAW**

SOLUTION PROVIDER: **BORDERLESS CS**

SERVICE: **DIGITAL / EMAIL FORENSIC**

Background: From June to July 2023, V1, V2, and V3 communicated via email to purchase bathroom materials for a renovation project. Invoices were exchanged, and payment schedules were discussed.

Incident Overview: During this period, one of the email accounts involved in the transaction was compromised. The hacker gained access to the account and leveraged the trust established between the involved parties. Using this compromised account, the hacker manipulated the legitimate invoice, altering the bank account details to redirect the payment for the remaining 50% of the invoice.

Deceptive Action: The hacker's forged invoice appeared identical to the original one, with the only noticeable change being the altered bank account details. The email was sent to one of the involved parties, and due to the trusted nature of their ongoing correspondence, they failed to notice the changes. This led the recipient to transfer the remaining payment to the hacker's account, believing it to be a legitimate request.

Discovery and Forensic Investigation: The issue was flagged when the legitimate supplier contacted V1, V2, and V3, noting the discrepancy in the payment received and informing them of the fraudulent transaction. A law firm brought in **Borderless CS to conduct a digital forensic analysis.**

The forensic team at **Borderless CS** conducted a thorough investigation, examining the email headers, metadata, and security logs. Through the analysis, they identified signs of unauthorised access to the compromised email account, including unusual login locations and timestamps. The manipulation of the invoice was traced to the time window when the email account was under control of the attacker.

Outcome and Recommendations: Thanks to Borderless CS's email forensic capabilities, the identity of the compromised email account was revealed. The team also worked closely with the law firm to assist in further investigation and court hearings.

Additionally, Borderless CS provided the following recommendations to prevent future incidents:

1. **Implement Multi-Factor Authentication (MFA):** All email accounts should have multi-factor authentication enabled to add an additional layer of security.
2. **Regular Training:** Ongoing cybersecurity training for employees to recognise phishing attempts, and suspicious activities and how verify payment details.
3. **Enhanced Email Filtering:** Using advanced email filtering systems to detect and block emails that exhibit suspicious patterns or manipulation.

4. **Payment Verification Procedures:** Establishing an internal process to verify all payment requests, especially those involving significant amounts, through secondary communication channels.

Through their advanced forensic expertise, Borderless CS not only assisted in tracking the breach but also helped strengthen the security posture of V1, V2, and V3 against future cyber threats.