

## CASE STUDY

# Business Email Compromise Leads to Data Breach



## COMPANY

UK Barrister Chambers

## REVENUE

£15M

## KEY COVERAGE

Breach Response

Even with Multi-Factor Authentication in place and regular phishing training, human error can still be the cause of a cyber attack.

Policyholders should always contact Coalition Claims if they feel there may have been an incident, even if it seems innocuous.

This barrister chambers had good security controls in place when they came on cover and our scans didn't pick up any critical vulnerabilities. They also provide regular phishing email training to their employees but unfortunately, an employee still fell victim to a sophisticated phishing attack, clicking on the link in the email, and verifying her details over the phone as part of the multi-factor authentication process. The firm quickly contacted Coalition Claims when they realised that phishing emails had been sent to their clients from the employee's email account, and clients had begun contacting them to verify legitimacy.

Forensic and legal experts were engaged immediately. Although initially this event looked like a standard business email compromise whereby the threat actor was looking to use the client as a springboard for a wider phishing email campaign, it was in fact discovered that the threat actor had used a tool to download the employee's entire mailbox, meaning everything contained within it was considered compromised. This included highly confidential and sensitive personal data belonging to solicitor firms and end clients for whom the barristers acted, case and trial information, as well as data relating to criminal, family and medical cases. This inevitably led to wider legal obligations and increased costs.

By immediately engaging appropriate experts, Coalition Claims was able to determine the extent of the incident and work with the client to help them manage the incident.

## Lessons Learned: Even with training, humans make mistakes

Even with Multi-Factor Authentication in place and regular phishing training, human error can still be the cause of a cyber attack. Firms that handle sensitive data and documents should ensure secure access controls and robust processes for client communication that do not rely on email alone. Policyholders should always contact Coalition Claims if they feel there may have been an incident, even if it seems innocuous.

The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law