

CASE STUDY

# FINANCIAL SERVICES



## CUSTOMER PROFILE

As one of the largest private financial services firms in Australia, this organisation operates with a highly-skilled team and holds large swathes of personally identifiable data and financial records of its clients.

## CHALLENGE

Recently, an employee of the firm resigned, accessing and downloading significant amounts of private client data, before exfiltrating it to their personal computer. The files contained over 200 individual client account designations, account numbers, personal financial information, and cash balances which the firm considers to be private information.


The ex-employee left the firm quickly, moving straight to a competitor. Once there, they began soliciting clients to make the switch. The ex-employee also waived their right to a 'good leaver' bonus - which provided extra incentive to honour the confidentiality and non-disclosure terms of their employment contract – so the financial services firm knew their contractual employment agreement restraints would be tested.

## SOLUTION

The firm began working with Cyber Audit Team (CAT) in 2019 as a client of CAT's Managed Detection and Response (MDR) services. While traditionally used to protect against threat actors and data breaches, MDR provides visibility into an organisation's entire digital environment and insights into user behaviour. MDR is an early detection and response capability that forms the cornerstone of cybersecurity maturity – the ability to Identify, Protect, Detect, Respond, and Recover from security events and incidents.

The firm's Executive team - in partnership with their lawyers - identified that the most immediate strategy to shut the ex-employee and their new employer down (deferring the more drawn out litigation process for enforcement of restraints) was to establish that confidential information had been removed from their systems, and to seek an injunction which would stop the use of this information. Leveraging CAT's MDR services and specialist skills, the team were able to definitively prove the firm's confidential data was accessed and retrieved from a non-work issued computer and IP address. CAT's Incident Report showed that not only had the ex-employee breached company policy by using their home computer to access company files, but had also contravened employment privacy terms. The information sourced from CAT enabled the financial services firm to successfully impose an injunction for theft of data / intellectual property on the ex-employee and their new employer in a matter of days.

CAT's MDR services were critical to the Financial Services firm taking effective legal action against the ex-employee and their new employer. The injunctive relief obtained as a result of the CAT analysis and data significantly limited damage to the firm's clients, brand, reputation and revenue.



CAT's MDR services have helped many businesses protect themselves, and their reputations, from external and internal threats over the years.

To find out more about our MDR solution, and how earlier threat detection through 'real time' monitoring can benefit your business, please visit our [website](#).

Cyber Audit Team is an independent Cyber Resilience Assessment and Managed Detection and Response Services provider.

The multi-disciplinary team of highly experienced industry specialists provide simplified end-to-end information security solutions as well as support and guidance to businesses of all sizes across various industries.

**Cyber Audit Team**

4 Helensvale Road  
Helensvale QLD 4212  
Australia

P | 1300 077 022

E | [enquiries@cyberauditteam.com](mailto:enquiries@cyberauditteam.com)

W | [cyberauditteam.com](http://cyberauditteam.com)

