ALTRAN

IRM INFORMATION RISK MANAGEMENT
A ALTRAN GROUP

FINANCE

Leveraging advanced red teaming for a leading UK challenger bank

CASE STUDY | STRATEGIC GRC TESTING

ABOUT THE CLIENT

The client is a specialist savings and lending bank based in the UK. Categorised as a challenger bank, the organisation is designed to serve the needs of SMEs and individuals in the UK and has now raised over £5.0 billion in customer deposits.

Since the bank's inception in 2011, it has invested heavily in securing its critical information assets, utilising the 'Big Four' to undertake regular risk assessments and a 'boutique' security testing company to check the efficacy of its internet-facing presence.

CREATING A BUSINESS CASE

Despite existing resources, during an investors meeting, IRM took the opportunity to present to the bank why it was critical for organisations to understand the real threat they faced; not just the industry perceived threat.

We demonstrated to the audience how data was harvested and how (using the dark web) its saleability meant that investment in cyber was misplaced by assuming the wrong threat actors.

A challenge was laid down by the bank's Chief Executive for us to conduct a red teaming exercise and to report to the board in four months' time.

APPROACH AND DELIVERABLES

Using the our Red Teaming methodology, we used techniques such as USB dropping, social engineering, undetected physical access, phishing, open source information gathering and rouge connectivity.

After 6 weeks, on 3 occasions, we managed to gain access to the building to plant devices connected to the network and gained full undetected access to all critical systems. We were able to gather HR payroll records, the M&A database, 750,000 credit cards as well as 1,500 customer bank and verification details.

750,000
credit card details accessed

The outcome of the exercise proved to the Board and the IT department that, whilst the obvious external facing systems were secure, there was sufficient elasticity in the physical and procedural security that enabled IRM to copy exactly how a serious and organised gang would operate. In addition, it showcased to the client the lack of detection in place.

1,500
customer bank & vertification details found

Since the exercise, presentations have taken place with the Board and Non-Executive Directors, leading the bank to make us their established security partner of choice.