ALTRAN

IRM INFORMATION RISK MANAGEMENT
ALTRAN GROUP

FINANCE

Cyber crisis management for a leading UK commercial bank

CASE STUDY | INCIDENT RESPONSE

Cyber Crisis Management Testing - Specialist Savings and Lending UK Bank

Context and Objectives

The client was looking to test the capabilities of different stakeholders within the business when dealing with an incident such as a cyber-attack or data breach.

To enable this, the client engaged with IRM to organise various crisis management workshops. At the request of the Bank's Head of IT Architecture and Security and Chief Risk Officer, IRM were asked to not lead or participate in the exercises, but deliver, facilitate and observe the exercises.

Setting the Scene

IRM based the cyber-attack on the following scenario:

- The Bank partners with another institution, increasing its public profile by 25%;
- Penetration tests identified a number of critical security vulnerabilities;
- Threat intelligence observed a higher than usual number of unsuccessful Denial of Service Attacks (DoS).

Challenges in the scenario included the Bank's website being defaced, the IT department being unable to fix the issue over the weekend and the website defacement being a diversion to a more serious attack.

We continued to present challenging issues throughout the incident response workshop, including rumours of cyber-attacks spreading on Twitter, the Bank's chairperson being approached by the media and a ransom demand of £50 million or the threat of customer's personal identifiable information being leaked on the internet.

Learnings

Following on from the exercise, IRM produced and delivered a report to the Bank. The report consisted of an Executive Summary of the key findings as well as the perceived current maturity level of the Bank (based on information drawn from ITIL, COBIT & ISO27035), written specifically for the Bank's Risk Committee. Further detail was then provided regarding each observation, along with specific recommendations for improvement.

IRM is working with the Bank on an improvement programme for their Cyber Crisis Management Plan and will be carrying out quarterly exercises of this nature, which are likely to increase in sophistication each time.