



Client

A FTSE 100 global broadcasting and telecommunications company

Project Background

The client was mandated to install a disclosure request system in order to conform to new EU data retention and existing UK Government RIPA requirements. The solution would automate and streamline the process of provisioning disclosure data for investigative purposes to law enforcements agencies as and when requested. Disclosure data comprises of extremely sensitive information such as call records, address details and credit card information which would be accessible via a single centrally accessed platform. As a result, securing this solution was paramount to preserving brand integrity and customer trust along with data protection compliance.

The system was developed by integrating commercial off the shelf products along with in-house developed components. Having captured various functional security requirements early on in the project, the client wanted to determine if the resulting solution implemented sufficient controls to safeguard customer data from malicious entities and that it fulfilled the security requirements chalked out by business. IRM was engaged to devise an approach that would shed light on residual threats, threats that were not identified during the design phase, validate them and recommend business friendly solutions for improving the overall security posture.

IRM's Approach

Based on project overview from kick off meetings, IRM was able to gauge that the system comprised of multiple data feeds, network services, databases, custom application code and hosting platforms. Owing to this complexity a standard penetration test would have been insufficient to cover every attack scenario, validate effectiveness of controls and determine adequacy of security requirements.

As a result, a multi phased approach was devised that leveraged IRM's capabilities in threat modelling and security testing. In place of black box penetration tests, all testing activities were driven by results of a threat modelling exercise that pointed out areas of concern in various components and aided in development of targeted test cases; ensuring maximum coverage of threat scenarios.

As with any business solution people, processes and technology were fundamental to functioning. It was imperative that the interaction of these elements with various components and underlying disclosure data was analysed to determine the true impact of each threat. IRM consultants had to engage with cross functional teams during the threat modelling phase, conduct interviews and carry out paper based review of design and processes. On several occasions IRM had to liaise with 3rd party vendors contracted by the client to in order to gain better understanding of the security architecture.

Once a satisfactory list of threats was developed, these were translated to penetration test cases targeting the network and application. Where potential risks associated with system builds were observed, IRM's build review services were used to compare the state of systems to common security standards and identify deviation from intended configuration.

As a result, IRM's unique risk assessment based approach analysed the requirement from a people, processes and technology perspective to identify gaps in the system and whether the existing controls were designed and implemented securely to protect disclosure data.

FAST FACTS

Geography

- ▶ UK

Challenges

- ▶ Protect stored customer data
- ▶ Ensure effectiveness of security controls

Solutions

- ▶ Threat Modelling
- ▶ Security Design Review
- ▶ Application Security Test
- ▶ Infrastructure Security Test

Results

- ▶ Holistic, unbiased, 3rd party verification of design and implementation
- ▶ Report that detailed vulnerabilities in the system along with remedial work required to safeguard customer data

Information Assurance

Risk Mitigation

Business Resilience

Compliance





What IRM delivered

IRM delivered a structured risk assessment and test report detailing potential risks and vulnerabilities which could have jeopardised confidentiality of disclosure data. This included reproducible test cases, remedial actions and details on additional development that had to be undertaken before the solution's go live date. Risks were abstracted into a high level threat scenario followed by vulnerabilities which could result in manifestation of the threat and finally a list of components that needed to be investigated for the presence of these vulnerabilities.

In terms of target audience, information was presented in an actionable intelligent form that enabled various stake holders, ranging from project managers to development teams, to make informed decisions.

Benefits to the Client

On completion of the engagement, the client had attained a holistic, unbiased, third party verification of design and implementation. Actions needed to ensure the system was compliant with various regulations and that disclosure data was being protected were clearly outlined. The client now had a list of threats, vulnerabilities, their business impact and the cost to remediate which was integral to making decisions.

Another added advantage of IRM's approach was that the resulting deliverables provisioned a baseline risk model of the solution. As a result, any changes introduced to the system could be easily incorporated into this model to determine the overall impact they could have to its threat profile and accordingly new test cases could be developed to carry out re-verification.

What the Client did next

On account of IRM's input to the project, the client was able to carry out necessary remedial action and introduce additional controls to safeguard disclosure data thereby conforming to applicable compliance requirements and inadvertently protecting brand integrity.

In terms of internal security processes, the client introduced security touch points during project initiation phases that enabled them to engage IRM early on in the project lifecycle thereby being able to pre-empt high risk areas and suitably guide development and test cycles to mitigate these risks.

Information Assurance
Risk Mitigation
Business Resilience
Compliance

