

Case Study: Penetration Test – Citrix**Industry Sector: Finance**

Citrix deployments are often utilised to provide restricted-functionality environments to internal staff and third-party organisations, including contractors and external consultants. If not adequately secured these environments provide a wealth of opportunity for the 'interested' or malicious user to gain elevated levels of access to networked systems.

Poorly-secured Citrix deployments can present a serious risk to finance and banking institutions by allowing restricted users to gain unauthorised and unaudited access to internal finance related applications and systems.

IRM identifies the security and business risks present within a Citrix environment to enable financial institutions to mitigate those risks to an acceptable level. IRM adds value to the penetration testing process by providing deeply technical business consultants who deliver findings in terms of the necessary business impact analysis to the information security managers who demand it.

Case #1 – Our commitment to delivering value

IRM was asked to perform a penetration test against the Citrix implementation of a global insurance and financial services provider. The Citrix environment was deployed to provide a reduced functionality desktop environment for third party contractors located in the providers' offices.

IRM identified that the third party contractors were able to gain access to restricted applications and personally identifiable data belonging to staff and clients through a misconfiguration within the Citrix environment. IRM was able to provide evidence that a contractor could gain domain administrator level privileges on the client network and full control over the Microsoft Windows based network; this included wholesale access to proprietary information held in a database cluster.

Due to the severity of the business impact as assessed by IRM, a full debrief workshop was arranged to present the recommendations within the report and to discuss prioritisation of the necessary remedial work. This assisted the client in attaining a significantly increased level of confidence in the security of their systems and confidentiality of their sensitive data in an appropriately structured and timely manner.

Case #2 – Our people are the differentiator

IRM performed a penetration test against the Citrix implementation of a global private equity group. The Citrix implementation had been deployed to provide remote working facilities to employees. Weaknesses in the controls surrounding the Citrix environment, combined with deficiencies in the corporate security posture as a whole, provided IRM with the opportunity to gain unauthorised access to critical network infrastructure.

IRM was ultimately able to gain domain administrator level privileges and thus effectively control the networking infrastructure, the VOIP telephone system, CCTV cameras and also a number of other less critical systems.

Following receipt of the detailed report containing technical recommendations to mitigate the risks, the client engaged IRM to conduct a formal risk assessment of a number of key components within the internal corporate infrastructure. IRM was able to draw from its experienced security management practice to provide the necessary resource with a strong background in the investment industry.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.