Technology Risk Assessment

Background

Our customer is one the leading microfinance bank in Pakistan. Headquartered in Islamabad, Pakistan, and operates in all four provinces including AJK & FATA through a large network of branches in three regions with over 100 plus branches. They desired to engage a consultant who could help them identify the risks posed to their IT infrastructure and provide a mitigation plan. INFOGISTIC was selected by client after a competitive bidding process.

Problem Statement

The client IT infrastructure was expanding day by day. With the expansion of networks and provisioning of online facilities to customers, they decided to conduct a 360 degree review of its digital boundaries. The technology risk assessment project which included internal and external penetration testing, web application testing, social engineering, security hardening reviews, data centre security, network security review, security policy review. They also desired to gauge the security awareness level of their staff at corporate office and branches.

INFOGISTIC's Approach

INFOGISTIC consultants conducted the vulnerability assessment to identify the potential weaknesses in the IT infrastructure and web applications. After due diligence with client team, selected vulnerabilities were exploited from internal and external interfaces. The penetration testing was conducted using the guidelines from OWASP (Open Web Application Security Project) & OSSTMM (Open Source Security Testing Methodology Manual). The Technology Risk Assessment (TRA) was conducted using the guidelines of NIST and ISO 27002. TRA included activities such as Network Security Review, Security Hardening Review, Social Engineering, Data Centre Review, and Physical Access Review. INFOGISTIC consultants also conducted the policy compliance review by reviewing the information security related policies and procedures in place. To increase the capability of the information security staff, trainings was also conducted which included workshops on Security Awareness, Developing Enterprise Security Frameworks and how to conduct vulnerability assessment and penetration testing. The recommendations were also made to client as part of the report on how to further strengthen the digital boundaries by implementing technology controls.

Benefits to Customer

Technology Risk Assessment provided a detailed insight to the client management about their existing information security state. The exercise helped them to reduce their risks related to information security. It provided a platform for the information security team to convey to other departments that information security is the responsibility of everyone in the organization hence they must follow the security policies and procedures.