



PROJECT GOALS & BENEFITS

- Validate that the fundamental design of the Application, (including Encryption mechanisms) were sufficient to ensure the confidentiality of key city employee confidential data.
- Identify potential risks/vulnerabilities relating to the city's hosting environment and their potential impact on the new application.
- Identify potential risks/vulnerabilities relating to the key processes relating to application development, change management, operations, system maintenance, and other key processes and their potential impact on the new application.
- Provide detailed reports covering identified vulnerabilities and ways to mitigate those risks.
- With recommendations executed the client signed off on the continuation of the project.

CASE STUDY

Application Security & IT Controls Assessment

When it came to the security of an application that held sensitive financial data on key elected officials, a major US city's application group turned to Pivot Point Security for an expert, independent audit of their application security and IT controls environment.

BACKGROUND

The client, a major US city's IT group, planned a phase one rollout of an application that would allow the public to search database of filings of the financial disclosures of several thousand elected officials, agency heads, and other government staff. This application was to replace a much older paper-based system. With the initial module rolling out in late 2004, they turned to Pivot Point Security to execute an independent review of the design of the application prior to its development. Concurrently, Pivot Point Security conducted a controls assessment of the key application support processes, hosting environment, and development methodology to ensure the resultant security of the application.

KEY PROJECT CHALLENGES & DELIVERABLES

With the sensitivity of the data transacted on the new system, security of the data during entry, from initial entry through database storage was critical.

- Assess overall level of risk relating to the large and complex surrounding IT infrastructure
- Review and advise on necessary changes to Systems Development Lifecycle Methodology to required control of critical development and deployment processes.
- Develop Test Case Scenarios for all major System points of attack (e.g., Web Server, Database Server, Application Server, Network Segment, Client Workstation, DNS Server) from multiple postures (e.g., hacker, domain user, administrator, developer, consultant)

- Develop Test Case Scenarios for all major Application Layer Attacks (e.g., Man in the middle, Cross Site Scripting, SQL/HTML Injection, Cookie Poisoning, Cookie Theft, Hidden Field Hijacking) from multiple postures (e.g., hacker, authorized user, administrator, developer)

ASSESSMENT/TESTING

On project kick-off, a team of Pivot Point Advisors, each with a particular specialty (e.g., Oracle, JAVA/BEA Web Logic, Web Development, Cryptography, Information System Controls, Network Architecture) met with client management to define key concerns and to establish a project timeline.

"With the sensitivity of the data transacted on the new system, security of the data during entry, from initial entry through database storage was critical."

The goals of the project were to assess the design of the application from all potential risk factors:

- The architecture of the application itself
- The surrounding technical environment in relation to the new app
- The operational support infrastructure for the



- environment and application,
- The administrative procedures for the client with the application.

In total, these assessments resulted in a comprehensive report delivered and reviewed with the client to detail any deficiencies that would need to be corrected prior to the application development and rollout.

The Pivot Point audit team conducted the audit from the perspective of both the business and technology aspects of the application. As IT security is a critical business issue, the team looked at the strengths of an enterprise from a personnel, processes, and technology standpoint.

Recommendations were made to:

- Implement improved private key management/storage mechanisms.
- Educate their community of end-users on their role in securing the application including client workstation security and password best practices.
- Mitigation of spyware, and social engineering (Phishing) techniques were also reported to supplement the controls assessment.

Utilizing the fundamental principles of application security: authentication/authorization, confidentiality, integrity, and non-repudiation, the Pivot Point team went to work to inspect the technical methods that the client was using to ensure application security. Using well-known vulnerability scanners and other tools used in ethical hacking, the Pivot Point team went to work to attempt to exploit the vulnerabilities they previously found. It was through this combination of vulnerability assessment and the substantive nature of their penetration testing that the Pivot Point Security team

were able to successfully meet the client's goals of optimum security prior to the application rollout. Encryption methods were reviewed and assessed accordingly and processes were recommended to ensure the optimal security of encryption methods currently used in the application test phase. External technology environment serving and supporting the application was reviewed and assessed and recommendations were made to management to continually validate that their rigorous Intranet application hosting requirements were being met. Specific additional technical recommendations regarding configurations of firewalls, VPN hosts/clients, two factor authentication, vulnerability monitoring and disaster recovery were also made.

Utilizing findings from the aforementioned as well as plentiful additional findings through out the course of the project, the Pivot Point Security team delivered a comprehensive report to management with advice on compliance with regulatory standards as a benchmark of security and governance as well as recurring audits to continually monitor the application's security.

GOOD NEWS

After the implementation of the recommendations in the final report the client was extremely pleased with the resultant security posture of the application. Key to their satisfaction was their achievement of the projects most significant goal:

"Ensure that the security of the application surpasses that of the old paper-based version it is replacing."



ABOUT PIVOT POINT SECURITY:

Achieving, and more importantly maintaining, a "reasonable & appropriate" security posture in today's environment requires a new approach. We approach IT Security as a business issue and focus on IT Governance, appropriate balance of key elements (people, process, & systems) and objectives (risk, cost, usability, and performance), strong control environments, and ongoing monitoring capabilities. Those safeguards are the hallmarks of today's best security architectures and the strength of Pivot Point Security.

Pivot Point Security is the premiere provider of information security auditing, penetration testing, enterprise security management, vulnerability assessment and mitigation services and solutions in the NY / NJ / PA metro area.

Clients (small business through international corporations) benefit from our Internal Control oriented approach to Information Security and our assistance with complex issues including Sarbanes Oxley, HIPAA, and SAS-94.