Infrastructure and Data Solutions

Case Study:

Information Security Governance Cyber Security Assessment Hospitality and Gaming Industry

Client Situation

A major hospitality and gaming company relies on its reputation as a secure entity. They wanted to know of any potential vulnerabilities in their networks, systems, and applications in order to evaluate their security program and their ability to respond to attackers. Since it is a publicly held company and accepts credit card payments, SOX and PCI criteria, as well as business best practices, were the accepted standards for evaluating the security level.

The criteria to establish and evaluate the impact and severity of an attack included such factors as:

- Lost revenue
- Loss of public image
- Failure to meet legal, regulatory, and/or contractual obligations

Experis Solution

After careful evaluation, Experis' Infrastructure and Data Services (IDS) practice was selected as the vendor to assess the security of the networks, systems, and applications. IDS provided services to measure and analyze network exposure to the company's network. Experis' experience with a variety of organizations has helped us create a suite of penetration testing, assessment, and security services.

IDS included vulnerability assessments and penetration testing services specifically tailored to the company's needs. Aspects of the execution and reporting were specific to the company's legislative and auditing needs. The focus of this project was to evaluate the security of systems and their vulnerability to external attacks. This included evaluating their susceptibility to penetration and subsequent compromise of internal systems containing sensitive PCI related data.

About Experis

Experis is a leading provider of customized IT staffing, technical and business process solutions with offices across major markets in the United States, Canada and Europe.

Now a ManpowerGroup company, Experis leverages their expertise by providing clients with a single source solution for highly skilled talent and technology solutions in the areas of IT, engineering, finance and healthcare.

Experis™ IT

Experis' IDS team completed the following tasks:

- Performed Vulnerability Assessment and Penetration Testing of the corporate network
- Provided a Gap Analysis and recommendations for risk remediation
- Presented report documentation that included specific formats, unique risk expression and matrix, complete mitigation strategies for any and all findings, relating to the "gap analysis" of findings vs. any legislation, standard or regulation applicable to the company

Experis performed testing services using baselines specific to the legislative and guideline requirements facing the company. PCI and SOX regulatory guidelines were taken into consideration with existing information security policies and used as a baseline standard for testing and reporting. This allowed the board, executive committee, or auditor to quickly understand the risks faced by the company and to understand the path to risk mitigation.

Client Benefits

- Formal prioritization of vulnerabilities and their potential impact allowed the IT department to accurately identify those servers and applications at greatest risk
- Provided management with an accurate understanding of which systems should be remediated first to maximize the impact on total network security
- Recommendations for support requirements for critical systems
- Established the minimum operating requirements for the system security
- Obtained formal management agreement, direction, and communication of the business risks associated with those vulnerabilities which were discovered and subsequently remediated

Contact us today to learn more about how Experis can help you grow your business through IT solutions.

experis.com