



Mitigating Risk at a Grand Casino in Asia

Consulting Overview

Business innovation today means extending beyond the enterprise through open collaboration and direct interaction with customers, tighter integration with partners, and the incorporation of external talent and resources. But without the right security strategy, innovation of this sort can make an organization's information resources vulnerable to loss and misuse. An information security strategy should be based on a comprehensive understanding of information assets, threats to those assets, current controls used to protect those assets, and the resulting risks.

To determine if their information resources are vulnerable, many companies and organizations begin the process with an independent analysis of their existing environment. An Information Risk Assessment Service from EMC is a broad-based security assessment designed to provide a systematic overview of an organization's management, technical, and operational controls along with a roadmap for risk remediation.

Recently, EMC® Consulting, part of EMC Global Services, successfully completed an assessment of information risk for a new grand casino in Asia. The information risk assessment was designed to uncover any potential security exposures in the new production servers and network infrastructure.

"The EMC information security consultants performed a thorough assessment of our new infrastructure," says the customer's IT department director. "With the latest in networking and wireless technology—and the trust of our customers, employees, business partners, and investors at stake—we cannot tolerate even the slightest defects in our security profile. EMC's rigorous approach to assessing vulnerability enabled us to take our security practices to a new level."

In the summer of 2007, the customer released a request for proposal (RFP) to conduct an information risk assessment of its information security solutions in the production environment. "EMC's response to our RFP evidenced extensive experience and understanding of information security practices as well as a good grasp of our business environment," says the customer. "We chose EMC over IBM because we believed its approach would ultimately provide the level of security we needed."

Information risk assessment

Working together, EMC consultants and the customer reviewed and revised the customer's existing security standards and policies to fulfill the requirements of Sarbanes-Oxley (SOX) compliance and ISO 27002 best practices. The goal was to understand both their business and IT operations and to recommend new security safeguards.

To begin the assessment, the EMC team reviewed the customer's network infrastructure by aligning and comparing it with EMC's security architecture standard.

EMC next turned its attention to scanning the network and system to detect potential vulnerabilities that would allow an attacker to gain access to the network or data residing on the network.

In one of the most exhaustive portions of the study, EMC assessed wireless network security and VOIP implementation. The team monitored the network perimeter for signal leakage, performed penetration tests, and emulated both a determined attack to access WEP encryption and a determined brute-force attack to recover WPA keys.

The EMC security experts also conducted a three-day ethical hacking service using typical black-box, pen-test activities including reconnaissance, scanning and enumeration, password guessing, and gaining access and escalating privilege.

Finally, the EMC team reviewed the overall firewall architecture to determine how effectively it isolated untrusted, outside networks from gaining access to the customer's internal, trusted networks and systems.

After completing the activities described above, EMC developed a risk and remediation roadmap of the customer's production environment. The EMC consultants identified areas of concern and recommended the new security safeguards that the customer should put into place.

The customer reports that the assessment findings were startling. "We thought that we had initially implemented a secure environment. But the EMC security consultants uncovered vulnerabilities that we never knew existed. Without this assessment, we would have gone live with a high degree of risk."

Ensuring security

Based on the results of the information risk assessment, the customer implemented the recommendations. The EMC team then performed a re-check on the security controls implemented and re-scanned the environment to ensure that the proper remedial actions had been taken.

"The fact that EMC came back to ensure that the vulnerabilities they had identified had been mitigated, gave us a high degree of confidence," says the customer.

"We have been operating our production environment for almost a year now and our security has been flawless," says the IT director. "I would urge any organization to invest in an information risk assessment of their vulnerabilities. The value delivered by EMC far exceeds the cost of the service." The customer continues to work with EMC Consulting, which recently conducted a Disaster Recovery Assessment and developed a disaster recovery infrastructure configuration plan.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

Take the next step

For more information, contact your local EMC representative, call us at 1-866-464-7381, or visit our website at www.EMC.com/consulting.