A ROADMAP TO AN ENTERPRISE INDUSTRY STANDARD OF SECURITY

IT Risk Management

Client Profile

A large manufacturer with facilities in more than 20 countries.

Challenges

One of the foremost challenges was the scope and Following an extensive RFP procedure—during which the client also considered IBM and Gartner for the project—CBI was selected to address significant concerns with the company's security posture. As a Fortune 500 organization of considerable magnitude, the company simply couldn't afford to maintain anything less than an enterprise industry standard of security. The CBI experts started at the base level with a comprehensive enterprise risk assessment. As part of the risk assessment, CBI facilitated strategic interviews of key decision makers and stakeholders in order to assess the effectiveness of various security policies and procedures.

The enterprise risk assessment uncovered IT inconsistencies across the company. As part of the risk assessment, penetration testing uncovered a wide array of threats affecting the organizations intellectual property that needed to be addressed immediately. A root cause of the plethora of security shortcomings was the lack of an organizational infrastructure. Due to other business related priorities and the organizations' structure, the company was unable to respond to and prioritize threats in a timely fashion. And serious security hazards were discovered in the form of malware, exposing the client to substantial risk of intellectual property and data loss.

Solution

In order to ensure that the client reached its goal of establishing an enterprise industry standard of security, CBI approached the project from several directions. Acting first and foremost as a trusted advisor, CBI had industry experts in the trenches, prepared to interpret the core trouble areas and provide detailed recommendations immediately.

Part of the assessment procedures included a Malicious Activity Assessment, identifying various forms of high-risk malware and botnets. CBI then provided a step-by-step plan to remediate the infections without causing network chaos. Once the security fires were extinguished, CBI worked with the client's IT team to better comprehend and utilize the software the company already had in place that could maintain network monitoring on an ongoing basis.

Finally, CBI provided the client with three tangible deliverables: a security roadmap, a vulnerability assessment report and a prioritization path. The strategic security roadmap provided a long-term, executable plan to move forward with security initiatives in a controlled, timely manner. The vulnerability assessment report provided the in-depth technical analysis of the various threats and risks identified during the penetration testing process. The prioritization path allowed the organization to implement recommendations outlined in the security roadmap in a prioritized fashion, understanding that certain recommendations needed to be conducted in a phased approach, scaling the course of three years. This allowed the organization to move forward with strategic recommendations given the threat to the organization, but also taking into consideration budget deliberations and the cost effectiveness vs. value to the organization. For example, a priority for 2012 is for the client to understand and define what data is considered classified within their network.

Results

The CBI solution has already delivered results that will play a critical role in the client's security posture for the foreseeable future—and that was just phase one of a multi-phase initiative. By providing a plan to extricate the malware and botnets with a methodical approach, the client's sensitive data and invaluable intellectual property will be secure from internal and external predators alike. CBI also assisted in establishment of a CISO, which will enable the manufacturer to proactively address potential threats before they become significant issues.

As a result of CBI's depth of knowledge and industry expertise, the client realized substantial cost savings by avoiding the purchase of additional monitoring software. Finally—and most importantly—the client is now on the path to an enterprise industry standard of security. Following the initial enterprise risk assessment, CBI was engaged by the client for a three-month project to remediate the upfront vulnerabilities.

OVERVIEW

Industry
Manufacturing

Solution
Malicious Activity Assessment (MAA)

CBI Generated Results

- Security of sensitive data and intellectual property
- Proactive mitigation of potential threats
- Substantial cost savings
- Set the client on a path to an enterprise industry standard of security

CBI CASE STUDY