

White Paper

Devfense Network Security Assessment: Return on Investment

devfense

network security assessment



There is value in a Devfense Network Security Assessment (NSA) that goes beyond the labor of creating a report to analyze a company's infrastructure to check for vulnerabilities.

For most SMBs and enterprise-class operations, a network assessment process that includes a physical walkthrough of facilities, infrastructure investigation, penetration testing, and other measures is essential for maintaining business continuity, protecting customers and maintaining security compliance.

Return on investment becomes realized immediately. Engaging professionals provides the benefits of proven methodologies, access to specialized tools, and practical insight, all garnered through experience. Following an engagement, returns are compounded as improved security posture and practices provide repeated cost-savings in IT performance and operations, not to mention the risk mitigation and the avoided costs of a security breach.

Cost of a Security Breach

Let us consider that the chance of a company suffering a data breach resulting from being a victim of the increased attacks of malware and/or, phishing schemes. Penetration into an organization's IT infrastructure resulting from Trojan viruses and keylogger software (to name just a few tactics) is certain in the absence of security measures.

The threat to business continuity from such attacks is well-demonstrated in the cases of some recent well known breaches, such as TJX in 2007, an incident that industry analysts expected cost \$1.7 billion. The estimate was based on assumptions including \$1.14 billion for customer remediation and an average cost per client record of \$37.

Meanwhile, we are still seeing fallout from the more recent Heartland payment systems security breach, which processes payments for more than 250,000 businesses. The full scale of costs for remediation and damage to Heartland's business is not yet clear, but it certainly has the potential to amount to hundreds of millions of dollars in costs.

This comes closely after the RBS Worldpay breach from December 23 2008. This breach of the company's payment systems has affected more than 1.5 million people and has resulted in at least a hundred fraud cases. The company was forced to offer one year's credit monitoring for at least 1.1 million of those customers.

The size and costs involved in these breaches may be difficult for SMBs to fathom. A more reliable measure is the Ponemon Institute's "Cost of a Data Breach" study, which put the damage of a breach at \$202 per stolen record.

To conduct a quick calculation of the cost of a breach to your organization, multiply Ponemon's figure by the number of records of your company. If you have tens of thousands, you can easily understand the reason to be vigilant with regular network assessments and the implementation of their findings.

Capabilities of a Network Security Assessment

A Devfense Network Security Assessment provides immediate value with a report containing priority network infrastructure recommendations. This will be used to improve and maintain business continuity and achieve regulatory compliance.

The unique approach includes:

- A comprehensive interview with IT staff as well as running an expanded set of internal and external tests on your network.
- Comprehensive security checks and analysis against a comprehensive list of attack signature including and not limited to SANS (SANS Institute Top 20), OVAL (Open Vulnerability Assessment Language), CVE (Common Vulnerabilities and Exposures – Mitre.org), and CVSS (Common Vulnerabilities Scoring System) threat classifications standards.

The final NSA report includes:

- Details of remediation tasks according to risk and effort level. Areas covered are based on the ISO 17799:2005 standard, such as access control, password policies, encryption, data classification, user account management, patch management, disaster recovery planning, security awareness training and backup systems.
- An assessment of IT policies, procedures and quality systems.
- Documentation of critical systems, including vulnerability and fix recommendations.
- A roadmap to prioritize your network security tasks.

Value of a Network Security Assessment

Most IT departments are too overloaded with user incident support or other essential tasks to commit dedicated effort to devise an approach that will balance the business and governance issues with the IT requirements.

To fully replicate in-house the capabilities of the essential network infrastructure security tasks undertaken with an NSA, a company would need to hire salaried network infrastructure and application security professionals, and purchase and maintain an arsenal of tools in-house. Even with these measures, the company would not be able to leverage the ever growing knowledge-base of good practices and security trends that specialized consultants supporting similar companies would be able to apply.

A company may only require NSA-type services on a quarterly or annual basis. Even if an in-house expert devotes three-to-six weeks focusing on security, the company would be required to pay their salaries for the remainder of the time, leading to unnecessary "mission creep" to rationalize their employment.

By engaging a security focused partner to assist the organization, companies will have access to a team of professionals, each focused on their area of expertise to develop a reliable solution. Furthermore, when you consider not only the salary of a security specialist but also the IT certifications required to maintain that individual's skills, and the licensing of tools and software to fulfill their security duties, costs would start upwards of \$150K. Outsourcing these tasks seems to be the more financially responsible approach.

An initial NSA engagement might cost as little as \$8,000, with subsequent quarterly engagements at an even lower rate. Even a robust deployment of Devfense NSA with regular monitoring, maintenance, and payment for additional vulnerability fixes, outlined by the NSA findings, could cost tens of thousands of dollars less than conducting these kinds of services in-house.

This is a huge value for organizations that increasingly need to prioritize spending of mission-critical revenue generating IT operations during a challenging economic climate.

The choice for today's companies is clear: outsourcing network infrastructure security with a PCIS Devfense NSA engagement is not only fiscally responsible but also provides better security.

About

Pacific Coast Information Systems Ltd.

Pacific Coast Information Systems (PCIS) Ltd. is a full-service technology and consulting firm based in Vancouver. Founded in 1995, PCIS offers packaged infrastructure and network solutions that enable organizations to address security and compliance issues within today's complex IT environment.

PCIS combines the specific tools, expertise and proven processes to accelerate the problem identification and resolution of security compliance thereby lowering business risk.

More information about PCIS can be found at www.pcis.com

Boonbox

Boonbox, a division of PCIS, was created in 2007. Boonbox provides solutions for identity management, data backup and recovery, and managed network services.

More information about Boonbox can be found at www.boonbox.net