A Guidance Consulting White Paper

P.O. Box 3322
Suwanee, GA 30024
678-381-1948
http://www.guidance-consulting.com

Eliminating Infrastructure Weaknesses with Vulnerability Management

By Guidance Consulting, Inc

Contents

Introduction

Threats today's companies face.

The Problem

The cost of a dedicated vulnerability management expert

The Solution

IT Consulting Firms

Finding professionals

Hiring Outside Consultants Versus Inside Staff

Vulnerability Management Program

Benefits to Vulnerability Management Programs

What to Expect

What to Expect from a Vulnerability Management Consultant

Eliminating Infrastructure Weaknesses with Vulnerability Management

Today, companies are facing even more threats to their IT infrastructure. Viruses, denial of service attacks, inside threats, and data theft are just a few of the ever-evolving methods hackers and technology thieves are using to attack businesses large and small.

No system is without flaws and weaknesses. However, with proper planning and assessment, any company can substantially reduce its risk of threat.

The Problem

After spending tens of thousands to millions of dollars developing a strong network, it can be difficult and costly to monitor a system's vulnerabilities and protect it on an ongoing basis. The cost to house a dedicated vulnerability management expert can be prohibitive, and each member of a company's IT staff has his or her own role to play aside from monitoring vulnerabilities.

Without a clear-cut plan of action in the event of disaster or attack, a business is at its most vulnerable, and this threat to security becomes a large liability that can result in lost income, lowered productivity, and lost reputation.

There have been several instances of customer information, such as credit card numbers or social security numbers, being breached. The impact this has on the integrity of a brand is immeasurable, and a company that doesn't properly strengthen its network to prevent this type of attack is sure to see a loss in revenue and customer support.

The Solution

IT consulting firms like Guidance Consulting serve to provide custom vulnerability management programs that monitor a company's system for weaknesses, eliminate them to strengthen the network, and plan proactively for future threats.

Sometimes, it takes a third party to truly assess an IT system and identify causes of vulnerability. Guidance Consulting uses an array of tools to provide quantitative results on how safe a company's information security is, including:

- Vulnerability Exploitation Tools/Penetration Testing
- Vulnerability Severity Ratings
- Vulnerability Scanners
- Vulnerability Tracking Metrics
- Vulnerability Tracking Documenting and Communicating

Once an infrastructure's weaknesses are identified, a vulnerability management consultant will work to develop plans, policies, and procedures that outline what to do in case of multiple types of attacks and disasters. This ensures the safety of the system.

With new viruses and attacks being developed nearly every day, only an experienced, qualified vulnerability management consultant can stay on top of them all and properly deflect them with appropriate actions.

Hiring Outside Consultants Versus Inside Staff

A question raised in the issue of vulnerability management is whether or not an outside vendor needs to be brought in to oversee and manage an infrastructure system. Certainly a company's IT staff understands the intricacies of the system. However, project managers, IT managers, quality analysts, and beta testers work on the day-to-day tasks and often don't see the bigger picture, which involves those areas of vulnerability that will be exposed to the risk of serious damage to a network.

A vulnerability management consultant works to assess a system's weaknesses, identify their causes, and eliminate the causes to ensure maximum security controls. Because the consultant sees the broad view, and because he or she has worked with numerous other systems and seen where the weaknesses lie, it can be easier to quickly determine areas of potential harm and create an effective plan to manage them.

A plan is the first step toward safety for any company. A consultant will document a management policy and detail step-by-step instructions to remediate any vulnerabilities that may arise down the road. Consider this insurance against viruses and attacks.

When it comes to cost, there is no price you can put on the safety and security of a business. However, vulnerability management firms are quite cost-conscious and work to deliver solutions that will save a company the large costs associated with infrastructure downtime, recovering from attack, and struggling to regain a lost reputation. A consultant will work with a business to develop a policy and implement it, and is paid for that time. Weigh this with having a full-time employee attempting to manage the vulnerability issues as they spring up in addition to managing his or her other tasks, and it is clear that there are cost savings to be recognized.

Benefits to Vulnerability Management Programs

The largest benefit to developing a thorough vulnerability management program is that it eliminates potential threats to a company's system. If a company's infrastructure is disrupted through denial of service attack, a virus, or hacking, precious customer data can be jeopardized. It can take days or weeks and thousands of dollars to recover the data and protect the system after an attack.

A vulnerability management specialist circumvents the costs of an attack by preventing them from occurring in the first place. Having policies and procedures in place before an attack ensures a lower likelihood of it happening.

Many companies recognize cost savings when they employ a vulnerability management consultant. Paying to take measures to secure a system is much more affordable than to try to recoup damages after the fact.

Another benefit to vulnerability management is peace of mind. Companies find they can spend more time focusing on business development rather than fretting over potential threats to their systems. A consultant handles the assessing, planning, and protecting while company executives can focus their attentions on matters they are more qualified to address.

What to Expect from a Vulnerability Management Consultant

A vulnerability management consultant will first start the process by assessing current policies and procedures a company has in place, if any. He or she will assess inventory and assign a value of importance to all assets to understand where the biggest threat to security lies.

He or she will then assess and classify vulnerabilities, including where and when they could occur to the infrastructure. He or she will correlate threats, including worms, wide-scale attacks, and exploits, and then determine a company's risk level based on all of these assessments.

The next step in vulnerability management involves cost analysis. A consultant will determine whether it is more cost effective to ignore vulnerabilities and risk attack or remediate the areas of weakness. There will be some necessary remediation for a given system, and a consultant will stress the importance of the investment in these.

A consultant will provide metrics by which an IT department can measure its system's vulnerabilities and policies for attack against a baseline and against ideal conditions.

He or she will help develop a plan to strengthen the network's weak areas as well as plan procedures to deal with an attack, should it occur. A strong vulnerability management consultant, like the ones at Guidance Consulting, will also provide ongoing training and communication to ensure the continued security of the infrastructure.

Safeguard Your Company

It's never been more important to protect your company's most valuable assets: your infrastructure. Guidance Consulting can provide you the peace of mind you need in knowing your system is safe from attack. Call us at 678-528-2681 to set up a complimentary evaluation to find out how vulnerable your system is.