A Practical Approach to a Comprehensive Security Program

— TruSecure Corporation

HURWITZ REPORT

Hurwitz Group

111 Speen Street

Framingham, MA 01701

T 508 872 3344

F 508 872 3355

www.hurwitz.com

HURWITZGROUP

HURWITZGROUP

A Practical Approach to a Comprehensive Security Program

— TruSecure Corporation

A Hurwitz Group white paper written for:
TruSecure Corporation
12379-C Sunrise Valley Drive
Reston, VA 20191-3422
Tel: 703 453 0500
Email: info@trusecure.com
Web: www.trusecure.com

Published by:
Hurwitz Group, Inc.
111 Speen Street, Framingham, MA 01701 ▶ Telephone: 508 872 3344 ▶ Fax: 508 872 3355
Email: info@hurwitz.com ▶ Web: www.hurwitz.com

April 2001

Executive Summary

The concept of security is frequently discussed in today's forums about technology and the Internet. Security is often cited as a critical issue that must be addressed in order to conduct business online. But many enterprises struggle with the challenges of achieving and maintaining an effective security posture, as indicated by the frequency of publicly reported security breaches.

TruSecure has created a holistic approach to security that provides organizations with an integrated, multifaceted program for understanding and reducing risk across the enterprise. TruSecure looks at the entire environment, assesses the risks, creates a plan for securing critical assets, and monitors the program over time. This process uses automated components for efficiency and human components for effectiveness to ensure that the program generates maximum risk reduction for the time and resources expended.

An Introduction to e-Business Risk

Risk is everywhere. It cannot be denied, only mitigated. Many risks are associated with daily activities like driving a car, playing sports, and investing in the stock market. The use of technology also has its risks. Identity fraud, denial-of-service attacks, and stolen information are but a few of the many risks associated with Internet and intranet activities. Because risks cannot be eliminated, appropriate steps must be taken to create an environment in which an organization is comfortable conducting business activities.

Technology risk is typically mitigated through the implementation of security measures. These security measures are designed to address a number of problems for e-Businesses. Risk is not just a theoretical construct; specific reasons to apply security measures exist, such as:

- **Protect critical assets**
- **Protect business reputation**
- **Regulatory compliance**
- **Due diligence for partners/customers/suppliers**

A risk-based approach to security management allows an enterprise to create a program tailored to match the chosen risk posture of that environment.

Security Tradeoffs

Tradeoffs must always be made when evaluating security measures used to mitigate risk. Like brakes in a Formula One car, when security is applied liberally it leads to laggard performance. Conversely, if security "brakes" are not applied at all it leads to an uncontrollable situation. In either case, the race is lost. Some of the more common tradeoffs to security are discussed below.

Connectivity vs. the Weakest Link

Many enterprises are extended networks of data centers, office facilities, and even home offices, any one of which can represent a risk to the entire network if its security is flawed. It is common for these enterprises to also connect to suppliers, business partners, customers, and supporting organizations. These connections foster real-time business transactions that have an immediate impact on an organization's success. But business partners connect with other business partners, and soon the network has turned into a massive patchwork of individual networks that rely on each other for security. In mutual-trust networks when trust is liberally applied, the strength of a security posture falls to the weakest component or environment. Ensuring a sound security posture across such an extended network represents a significant security management challenge.

Enabling e-Business vs. Absolute Security

Often, security professionals profess to enable e-Business in one breath while saying "no" to a network configuration request for some business opportunity in the next. The tendency is to take an absolute stance about security requirements — if some remote risk exists, it becomes too much for any initiative. A successful security program will take an approach to security that is reasonable, with the realization and understanding that the ultimate goal is to add to an enterprise's ability to conduct business online.

Security Issues vs. Security Resources

With IT budgets under continuing scrutiny, the pressure to deliver maximum return on security investments is high. Even in the face of reasonable security requirements, organizations must evaluate their ability to effectively address them. With limited resources, including time, budget, and skilled people, companies must work to address the security needs in their environments. The need to assess, prioritize, and possibly outsource functions that may be critical to success yet unattainable due to these resource limitations is real. The complexities of determining which security issues warrant time and attention are frequently beyond the scope of internal IT staff.

A Risk Management Approach to Security

Security works best with an approach that is comprehensive and sensible. It identifies risks for a particular environment and creates a life-cycle approach to managing the controls necessary to mitigate those risks. TruSecure has created a multiphase process (see Figure 1) to identify the computing components, assess the risks of the systems, protect the systems, and then assure the ongoing effectiveness of the program over its lifetime. Each of these phases is discussed below.

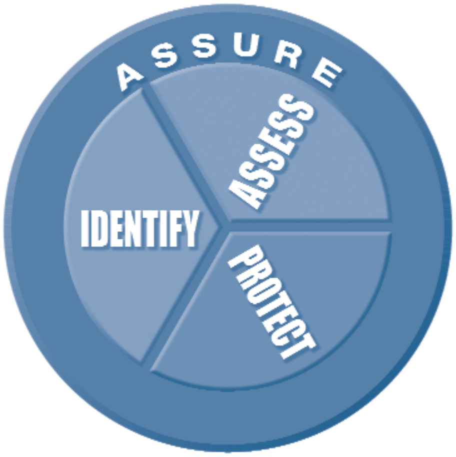

Figure 1. Four-phase approach to security.

Phase 1 — Identify

Overview

Any comprehensive security program must begin with the identification of computing assets. The TruSecure approach involves interviews of appropriate personnel and includes active and passive scanning of the network itself to identify "unknown" systems. The data is analyzed using both automated and manual means, then verified by an organization to provide detailed information about the networked environment.

Significance

Identification seems trivial, almost boring, but any network of decent size is bound to have misconfigured network segments or contain systems that are unknown and unsupported by information systems personnel. Often, these systems are significant assets to the organization. Human resources, finance, and corporate security all commonly maintain their own servers that could have significant security considerations. The initial identification phase provides a foundation on which to evaluate the entire environment without leaving out a critical asset or network segment.

Differentiation

The TruSecure approach is an efficient one. It uses automated tools to gather information and further refine it into the foundation for security activities. This automation serves two purposes: First, it is more efficient because the data can be used and further reused in the process. Second, it is more comprehensive because it uses automated scanning to detect systems that may have gone unnoticed by affected personnel. This approach helps to identify rogue systems that could pose a serious security risk.

Phase 2 — Assess

Overview

Once the total environment has been identified, its systems must be evaluated and prioritized. In addition, the systems must be tested for weaknesses to determine if vulnerabilities exist. TruSecure uses remote and local scanning techniques to identify these vulnerabilities. Onsite visits ensure that serious vulnerabilities are reviewed and confirmed.

Significance

A full assessment evaluates the defensive posture, highlighting weaknesses that may be probed and exploited to gain access to systems. It also provides priorities and information about more significant risks, to provide some sense of the importance of a particular risk.

Differentiation

The TruSecure approach focuses on remediation of problems, not their symptoms.
For example, rather than highlighting multiple situations that can be resolved with a single system patch, the focus is on applying the patch to gain the maximum coverage. The results from this step are prioritized to ensure that attention is given to the most significant issues first and then follows the list of priorities in decreasing order. This ensures that major security risks get addressed in all areas, including physical security, human weaknesses, privacy issues, and other current topics in security.

Phase 3 — Protect

Overview

Even mature security programs start to falter when it comes to protecting assets.
This is the area where users and data owners get involved in the tradeoff between access to their applications and appropriate security. TruSecure's approach presents a comprehensive risk reduction program to successfully manage the security posture of a particular

environment. This approach can be applied to multiple layers, including physical security, network security, operating system security, and services (application) security. In addition, the approach addresses the "human factor" that is often exploited through social engineering and misplaced trust.

Significance

This phase provides the controls that must be in place to ensure a proper security management program. It identifies and prioritizes issues, creating a user-friendly "to-do" list that contains all the descriptions and options for remediation for a particular risk. The approach is comprehensive and multifaceted to ensure security coverage throughout the enterprise.

Differentiation

TruSecure leverages its significant knowledge base to create a set of essential practices that identifies the appropriate security posture for a particular industry or market segment. One of the more valuable aspects of this approach is that it is realistic. The approach does not recommend products or tools, but rather provides alternatives for remediation that address a particular risk with a particular focus on leveraging the people and products already in place.

Phase 4 — Assure

Overview

It is a misconception that security is ever "done" when, for example, remediation of specific vulnerabilities is complete. New systems come online constantly, new vulnerabilities are identified, applications are deployed in different ways, and organizational changes occur frequently. Maintaining a security program involves collecting and analyzing existing data, such as CERT Advisories or other vulnerability warnings, and identifying those environments that may be affected. This information is evaluated, a solution is identified, and then it is sent to the appropriate organizations.

Significance

Any security approach must be ongoing. The technology world is constantly changing and security postures change along with it. Managing a security program forces a business to constantly monitor information and sift through it for applicable issues.

Differentiation

TruSecure provides a targeted alert system so that information about a vulnerability in Sun Solaris, for example, will be passed along to those customers with Sun Solaris platforms.

In addition to this vulnerability information, TruSecure adds its own analysis and steps that must be taken to address the risk. The ability to provide actionable guidance ensures that a weakness is addressed within a minimal time period, thus limiting the extent of the exposure. In addition, the process provides for recurring risk assessments to discover and address any vulnerabilities that may have emerged in the environment.

The TruSecure "Glue"

TruSecure puts these phases together into a comprehensive security program. The "glue" behind this holistic approach is rooted in the following features:

Extended Enterprise Management

One or many sites can be managed from a single console that provides management information with drill-down information for administrators and engineers. This information comes complete with a task plan, responsibilities, and timelines so the program can be managed and measured.

Integration of Essential Components

It is common to perform pieces of the steps described above within the scope of many other responsibilities. However, a piecemeal approach falls victim to point solutions that fail to demonstrate the strengths and benefits of a comprehensive program. An assessment that identifies vulnerabilities is a laundry list with no value when it isn't prioritized against critical assets and security impact. These assessments often don't lead to control implementations because of scarce resources, and all is for naught if a rogue system exists that undermines the entire strategy. An integrated risk management program is effective and manageable for any environment.

Resource Prioritization

Resource availability is a constant issue in the security space. Frequently, the bandwidth required to perform security functions gets lost in the midst of the latest antivirus attack, a senior management request for advice, or an investigation. A pragmatic approach to security provides essential practices that can be prioritized and implemented with minimal pain and maximum gain. This prioritization provides direction so that resources can be deployed for utmost effectiveness.

Dynamic, Custom Risk Assessment

The ability to take global security information and boil it down to specifics to be applied to a particular environment creates a custom approach to a broad problem. TruSecure strengthens this approach through its patent-pending, object-oriented security model. This methodology enables an assessment of risk that incorporates the relationships and dependencies between devices, data, users, and physical locations; it then targets security controls to address that specific combination of attributes. Following this approach maximizes cost-effectiveness by targeting the limited security resources in the right areas.

PHH Vehicle Management Services is a global leader in leasing, management, and card payment solutions for corporate, government, and utility fleets. PHH selected TruSecure after learning that TruSecure offered an innovative approach to managing complex network security environments, where multiple security technologies often coexist. PHH has been working with TruSecure for several years, and has seen significant business benefits from TruSecure's process.

"We can now demonstrate on a continuous basis to our partners that we have taken and continue to take due diligence measures to ensure the security of our operations at PHH," says Tim Talbot, Vice President of Information Technology Services at PHH. "So, this approach greatly contributes to the growth of our business."

Talbot and his team saw immediate value in TruSecure's program. "We were able to identify areas where we could improve upon, not only in the technical arena but also around our procedures and policies. It is a very rigorous and very thorough, continuous security assurance solution," says Talbot.

"Plus, it is just good business practice to incorporate continuous security assurance services into the daily running of an enterprise."

(source: TruSecure Corporation)

Business Model

TruSecure offers this security management program on a fixed-price basis with 24x7 annual support service included. Skilled security professionals that can define and manage the strategic security needs of an enterprise are a scarce resource. TruSecure's professionals come with experience, learn from situations at varied environments, and apply them in a strategic security plan.

Conclusion

TruSecure has married the old with the new by leveraging "tried and true" risk management approaches with a unique, online capability that implements an efficient strategic approach to security. Many environments struggle with reactive security issues and an ad hoc approach to security practices that results in missing pieces, open weaknesses, and an ineffective security program. The TruSecure approach brings a time-tested process online to provide for efficiencies of scale that result in a higher level of security for participating organizations.

translating technology into business success