HURWITZGROUP

Proactive Enterprise Risk Management

— Xacta Corporation

Hurwitz Report

HURWITZGROUP

Proactive Enterprise Risk Management

— Xacta Corporation

A Hurwitz Group white paper written for:

Xacta Corporation
19886 Ashburn Road
Ashburn, VA 20147
Tel: 877 40 xacta
Web: www.xacta.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

September 2001

Executive Summary

Today's Internet economy has forever changed the way the world conducts business. At no other time in history has technology opened the doors to new markets at a faster pace. While e-Commerce presents tremendous opportunities, it also introduces an enormous amount of risk. After all, the same technology that connects companies to the global marketplace also makes their systems vulnerable to attack.

As organizations leverage computer networks and the Internet to scale their businesses and be more competitive, directors and managers must understand the new risks introduced and the responsibilities assumed by opening their critical business systems and data to a public network. Regulations, guidelines, and standards are emerging to help companies define and implement appropriate security and privacy practices. However, without a reliable mechanism for frequently assessing and improving compliance with these standards, there is no prudent way to strike the appropriate balance between the risks assumed and the additional opportunity realized through e-Business initiatives.

This paper focuses on the concepts of security assessment and enterprise risk management. It introduces the Hurwitz Group model for securing an enterprise and describes the business case for security compliance assessment. The paper highlights Xacta Corporation's Xacta Web C&A™ and Xacta Commerce Trust™ solutions, and analyzes the role that automated compliance software plays in today's Internet economy.

Overview: The Hurwitz Group Security Architecture Model

Security can only be evaluated by better understanding the tools and processes that dynamically interact to protect the computing environment. This interaction should occur in a way that is appropriate for the sensitivity of the environment's data or the function it provides. Hurwitz Group's security model takes into account this dynamic nature of security (see Figure 1 below). It is intended to provide a flexible, reasonable way to evaluate an organization's risk posture. When a company applies Hurwitz Group's model to its security environment, the strengths and weaknesses of the environment will become apparent.

This model describes the types of controls that make up an effective security program. Due to the complexity of systems, these controls must be evaluated and reviewed at many platform layers, such as operating systems, databases, and the many enterprise applications.

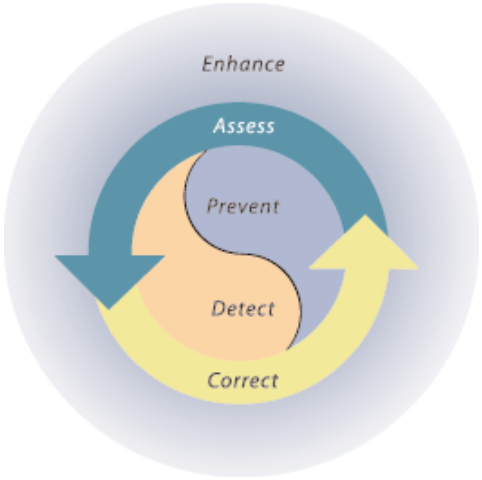

Figure 1. Hurwitz Group security architecture model.

- **Preventive controls** stop inappropriate activity before it occurs.
- **Detective controls** track security events after they occur and provide information for investigations when an incident is noticed or data is missing or corrupted.
- **Assessment controls** identify weaknesses in the environment by evaluating system configurations, security settings, access control lists, and other security elements of a particular system or layer.
- **Corrective controls** are measures that strengthen a computer resource or environment.
- **Enhancement controls** are structures and frameworks that are put into place to assist in managing a computing environment.

This paper identifies the major issues and requirements associated with these controls and then discusses how one firm addresses them.

The Business Case for Security Compliance Assessment

Requirements for Effective Security Compliance Assessment

Security managers realize the importance of security compliance assessment. Nonetheless, a number of questions remain when investigating alternatives for security compliance assessment, such as:

- How to select the appropriate security/privacy standards, regulations, and best practices pertinent to an organization
- How to assess and evaluate security posture by automatically detecting deviations from that standard
- How to prioritize risks based on these deviations, understand their potential impact, and take action to remedy them
- How to continually monitor, manage, and improve risk posture on a frequent and ongoing basis
- How to generate documents that address certification and accreditation requirements and summarize evaluation findings

Government (local, national, and international) attempts at establishing or influencing these requirements are prevalent in today's security environment. Let's first look at a few mandates that are in place today, extract their essence, and then extrapolate them across all industries.

Meeting Existing Mandates for System Security

HIPAA, Gramm-Leach-Bliley, and various Executive Orders are government-mandated requirements for security and privacy requirements in the healthcare, financial services, and government industry arenas, respectively. For example, every department and agency within the federal government has been mandated, by Executive Order, to develop, monitor, and manage an information security program. Such a mandate requires implementing a security policy and a process for certifying and accrediting that systems and networks comply with that policy. This typically manual and arduous certification and accreditation (C&A) process must be completed every three years or after each major system change.

In the absence of specific regulations, organizations in many nonregulated industries are now reviewing international standards as a starting point for defining appropriate security and privacy practices. International security compliance standards such as BS 7799 and ISO 17799 are being proposed as candidate standards for security compliance. In addition, de-facto standards bodies such as VISA are starting to publish security guidelines; if these guidelines are not implemented, VISA merchants risk losing use of the VISA logo. The implications are that companies may now have to include a compliance review for multiple, potentially conflicting mandates, have a policy for determining which standard to follow, perform an analysis of the cost of compliance, as well as noncompliance, with government standards in the countries where they do business, and evaluate the trade-off of complying with these standards.

Going Beyond Mere Compliance

Moving forward, mere compliance with emerging industry standards will simply be recognized as meeting minimum requirements and will not provide a safe harbor against loss. Minimum security compliance will not meet management's ever-increasing fiduciary responsibility to their shareholders, or their legal and regulatory liability for protecting their companies' information technology assets and their customers' personal data. As the awareness of cyber crime increases, the compliance standard will continue to be raised and organizations will be expected to go beyond minimum requirements and undertake all commercially reasonable steps to proactively monitor and manage risks. Furthermore, as the online presence of organizations increases, companies will be forced by their trading partners to "raise the bar" for minimum security compliance or risk being kicked out of lucrative online marketplaces.

A Snapshot in Time Means Nothing

Many companies have begun to embrace the concept of periodic risk assessments, possibly as a result of the Y2K experience or in response to increasing media coverage of security breaches. Some of the more proactive organizations are even conducting semiannual or quarterly risk assessments. However, an organization's security posture can change on a day-to-day basis due to system configuration changes, new e-Business initiatives, new vulnerabilities, and a host of other causes. Such changes, individually or collectively, expose the organization and can have a serious impact on risk and compliance posture.

You Need the Videotape

For this reason, organizations must begin to view enterprise risk management as a part of their own day-to-day business practices — not as a task to be outsourced or neglected — and should implement an iterative process that allows for continuous risk management. After all, when it comes to system security, a "snapshot" in time is inadequate. You need the "videotape."

Xacta Corporation and the Xacta Solution

Xacta Corporation, a Northern Virginia-based security software company, offers Xacta Web C&A to address the need for standards-based security assessment and will soon release Xacta Commerce Trust, a continuous enterprise risk management product. By leveraging Xacta Web C&A's Protect engine and the knowledge base the company created to support the system certification and accreditation needs of the federal marketplace, Xacta is enabling security-conscious organizations to go beyond mere compliance and take a more proactive, enterprise-wide approach to risk management.

Established in February 2000, Xacta Corporation employs approximately 120 professionals across the country with principal business offices in the Washington, D.C. and New York City areas. Formerly part of the e-solutions division of Telos Corporation, Xacta is now organized as a wholly owned subsidiary of Telos, one of the premier suppliers of network integration and systems development solutions to the Department of Defense and civilian agencies.

Xacta's innovative products leverage extensive consulting experience, domain knowledge, and best practices implementation in enterprise security. Xacta has proven its technology in the federal marketplace, where stringent security requirements and regulations have been the custom and practice for many years.

Xacta's enterprise security consultants have been ensuring that the government's demanding and security-conscious organizations comply with existing and emerging mandates for more than 10 years. Like many other consulting organizations, Xacta has provided C&A services on a time-and-materials basis. Through experience and discipline, Xacta honed the process and testing methodologies and began packaging these best practices as turnkey C&As on a firm, fixed-price basis in late 1999.

Xacta Web C&A: Automated Security Certification and Accreditation

In August 2000, the company took the next logical step, introducing Xacta Web C&A, the first commercially available software application that helps automate the federally mandated C&A effort. This database-driven technology enforces a consistent, repeatable process for every C&A performed. As a result, Xacta Web C&A enables organizations to identify and address vulnerabilities across and throughout their enterprises. Xacta Web C&A software simplifies certification and accreditation and reduces costs by guiding users through a step-by-step process to determine risk posture and assess system and network configuration compliance with applicable regulations and industry best practices.

Xacta Commerce Trust: Enabling Proactive Enterprise Risk Management

Xacta is significantly expanding the functionality of its initial product offering to create a continuous risk management system called Xacta Commerce Trust. This next-generation product makes it easy for organizations to go beyond mere regulatory compliance by understanding what standards should be applied; identifying, prioritizing, and addressing deviations; and managing risks on a continuous basis. As a result, companies can strike a balance between risk management and business opportunity as they scale their businesses to leverage the Internet and stay competitive (see Figure 2).

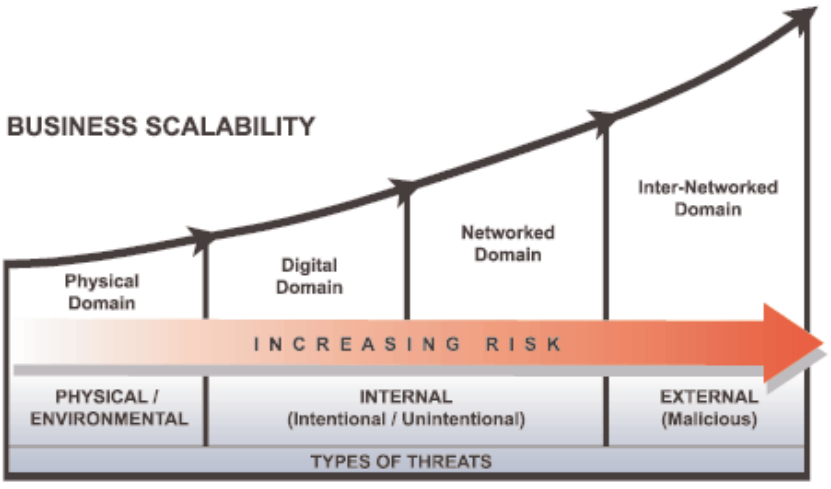

Figure 2. Evolution of technology: Introducing tremendous opportunity AND risk.

Simply stated, the various Xacta Commerce Trust functions are designed to empower an organization to:

- Define how its system should be measured by selecting the appropriate standard(s) from the software's knowledge base (content library)
- Determine the system/network's current risk posture (actual)
- Compare the current status with the standard (or target) to automatically identify deviations and their possible impact on risk posture
- Prioritize and act on detected deviations
- Continually assess risk posture against the chosen standard.

Xacta Commerce Trust also includes flexible reporting and publishing utilities that provide users with documentation and graphical reports to meet the information needs of the organization, from the system/security administrators through senior managers and directors. For the technical staff, these reports provide detailed assessment, testing, and evaluation results. For the executive team, they provide enterprise-wide visibility into detected risks and vulnerabilities, and insight into the business implications of such shortcomings. The information provided can be used to prioritize risks based on the severity of the threat posed, to identify countermeasures, and to estimate the cost associated with remediation.

The product architecture and specific functions are described below in more detail (see Figure 3).

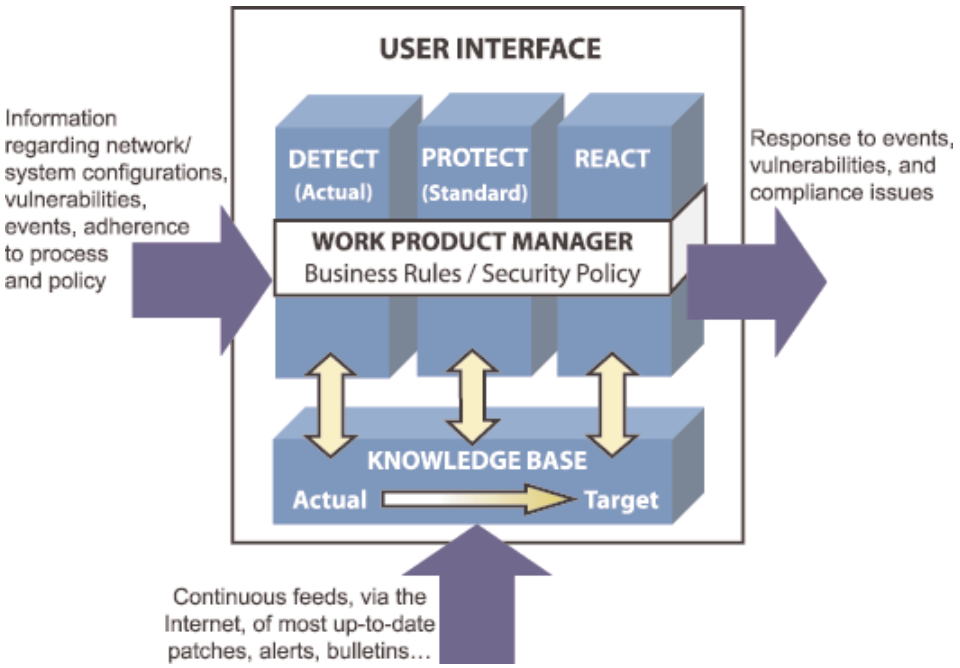

Figure 3. Xacta Commerce Trust Architecture.

Stage 1: Protect

Overview

Protect is the heart of Xacta Commerce Trust. The Protect engine was designed to help users define, select, or even customize appropriate risk measurement standards, i.e., which security requirements are relevant based on your business, industry, and sensitivity level. As you answer questions about your system and its environment, the appropriate requirements are selected from the knowledge base (content library) so that a security requirement's traceability matrix (SRTM) can be established. Once the system develops the SRTM, Protect then generates appropriate test plans and procedures based on the standard(s) chosen. This matrix, or association of system components, environmental factors, and measurement standards, forms the basis for the entire risk management process moving forward.

Significance

Building the SRTM and determining the test procedures required is a tedious, complex process normally requiring the expertise of a security and privacy regulations expert. Protect automatically generates this matrix based on answers to straightforward questions about your systems/network, the sensitivity level of the information that resides there, and the environment in which it operates. Additionally, evaluation criteria and processes (e.g., test procedures) that map to the requirements as specified by the standard are automatically developed.

Differentiation

This requirements definition and baselining process is automated to provide maximum efficiency so those responsible for security can limit the logistics effort required. As a result, organizations no longer need to delay their implementation of risk monitoring and management processes due to personnel bandwidth issues. In addition, the risk measurement standard developed by the Protect engine is based on industry-accepted standards, NOT proprietary "best practices" that may or may not be of relevance to specific industry requirements and mandates. The knowledge base also provides the power and flexibility to allow organizations to customize the standards to meet their specific needs and security requirements.

Stage 2: Detect

Overview

The Detect engine automatically performs an IP mapping of the current or actual environment, inventories hardware and software associated with each IP address, and performs comprehensive vulnerability scans. All of this information is ported to the Xacta Commerce Trust knowledge base and drives an automated risk assessment process. Upon completion of the initial baselining effort, Detect is used to check for additions, changes, and deviations from the defined measurement standard.

Significance

The Detect engine enables automated and continuous review. Continuous review is more valuable than a fixed snapshot in time. Additionally, these automated functions reduce the manual efforts

associated with gathering and organizing the extensive amounts of asset information and vulnerability data required.

Differentiation

Many enterprise management and security companies offer asset management, inventory management, and vulnerability assessment functionality. These are built in to Xacta Commerce Trust, so you can eliminate the need to invest in these other applications that are typically expensive to purchase, install, and maintain. In the event that you have already invested in such technologies, however, the open architecture of Xacta Commerce Trust allows you to leverage the information gathered by these other systems to populate the Xacta Commerce Trust database.

Stage 3: React

Overview

React, in conjunction with the software's Work Product Manager functionality, serves as a workflow engine that effectively allows organizations to automate critical risk assessment and enterprise risk management processes. As differences are identified between Detect (actual) and Protect (measurement standard), specific workflows are activated based on logic triggers. Xacta Commerce Trust incorporates standard process flows that can be customized to meet the needs of an individual organization.

Significance

React effectively automates security policy and practices by flowing information and directions to the appropriate parties, based on discrepancies identified in the environment by Detect. Workflows can also be activated, based on time triggers, to inform or remind members of the organization when it is time to take action on a specific security policy.

Differentiation

With React, security policy isn't a thick sheaf of papers that sits on a shelf. Rather, it becomes a proactive and automated part of your overall business process and is easily implemented and enforced to enable effective risk management across your enterprise.

Xacta Empowers the User

To effectively perform point-in-time or continuous risk assessment and management, it is necessary to collect and process an extensive amount of sensitive information — information that describes your business, business systems, and business processes. Hurwitz Group believes that this sensitive information needs to be owned, managed, and maintained by the business owner or a trusted partner, since outsourcing such a function introduces a different set of risks. It must be incorporated into an organization's best practices, policies, and procedures. To this end, Xacta's software is hosted in the customer's environment and is offered on a subscription basis. The subscription-based business model allows customers to

access information and resources that are constantly updated, such as security policies, regulations, test procedures, test tools, documentation templates, security alerts, and bulletins. To further support and empower its customers, Xacta has also created a wide range of services, which, in addition to product training, include mentoring services and online consulting.

Xacta Mentoring Services

Xacta consultants, or participating partner organizations, work side-by-side with customers to achieve rapid results. This mentoring activity is intended to be a short-term effort allowing customers to quickly define protection profiles and evaluation criteria, establish a baseline assessment, and establish a mitigation plan.

Xacta Online Consulting

Xacta also offers unique online consulting capabilities, providing customers with access to security experts via chat and email to provide guidance on a real-time basis. This service is typically hosted and supported by Xacta. If required, the online consulting console can also be hosted within the customer's facilities or within the customer's environment.

Hurwitz Group's Analysis

Security comprises multiple dimensions and is inherently dynamic. As companies start to adopt more automated assessment and response models like Xacta's, they need to keep the following in mind:

- How frequently are my information feeds about threats and appropriate responses being updated? Responding to yesterday's threats is no more effective than the Maginot Line was at the dawn of WWII.
- How frequently are the business imperatives of the firm being mapped to the underlying security infrastructure? Companies need to make sure that any new e-Business initiatives are analyzed for their impact on the security infrastructure and that threats are incorporated into the existing security response framework.
- Do I have the appropriate resources to effectively monitor and respond to all security compliance deviations? Many organizations seriously underestimate the manpower required to effectively respond to all security threats.
- Is senior management kept in the loop? Security issues are often unintentionally de-emphasized by senior management based solely on a lack of awareness and understanding.

Conclusion

Xacta's software and information assurance expertise has been proven in the government's most stringent security environments. With Xacta Commerce Trust, the company is leveraging its experience to provide the commercial marketplace with a powerful, proactive enterprise risk

management solution that enables organizations to measure and manage risk in accordance with industry standards and best security practices. Hurwitz Group anticipates companies will benefit by:

- Making more informed business decisions based on a comprehensive understanding of risks and vulnerabilities
- Protecting critical information assets
- Safely utilizing computer networks/systems to gain competitive advantage and capitalize on the promise of e-Commerce
- Complying with regulations and emerging security/privacy requirements and guidelines
- Increasing the productivity of their internal IT resources and reducing their reliance on security and policy experts

About Hurwitz Group

Hurwitz Group, an analyst, research, and consulting firm, is a recognized leader in identifying and articulating the business value of technology. Known for its real-world experience, consultative style, and pragmatic approach, Hurwitz Group provides strategic guidance to its clients by delivering analysis, market research, custom content, and consulting services. Clients include Global 2000, software, services, systems, and investment companies.

111 Speen Street Framingham, MA 01701 T 508 872 3344 **F** 508 872 3355 www.hurwitz.com