

Managing e-Business Risks

— Tivoli Systems Inc.

HURWITZ REPORT

Hurwitz Group

111 Speen Street

Framingham, MA 01701

T 508 872 3344

F 508 872 3355

www.hurwitz.com





Managing e-Business Risks

— Tivoli Systems Inc.

iii Executive Summary

As a greater percentage of business transactions move online, a company's information assets have taken on greater importance with regard to business success and, at the same time, have become more vulnerable to attack than at any time in the past.

2 Why Risk Management?

As companies embrace e-Business, they are faced with a new and large set of risks.

3 How to Manage Risk

To responsibly engage in e-Business, companies need to manage electronic risks as a part of their business model.

3 Security Products — Risk Mitigators

A well-architected e-Security solution should be more than just a collection of point products.

4 What Can Be Done About This?

To remedy this situation and maximize the effectiveness of its security defenses, companies need to provide a scalable event management platform to integrate and manage security products and correlate the information they provide.

5 An Example Solution — Tivoli® SecureWay Risk Manager®

Tivoli SecureWay Risk Manager is the result of Tivoli's attempt to define the requirements of enterprise risk management, and it provides an impressive set of capabilities.

8 Conclusion

In Tivoli SecureWay Risk Manager, Tivoli provides centralized management of security products with an intelligent engine to improve responses to threats — and analysis and reporting to enable better understanding of risks and provide a basis for improving the security architecture.

A Hurwitz Group white paper written for:
Tivoli Systems Inc.
9442 Capital of Texas Highway North
Arboretum Plaza One
Austin, TX 78759
Telephone: 512 436 8000
Fax: 512 794 0623
Web: www.tivoli.com

A Publication 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

October 2000

© Copyright 2000, Hurwitz Group, Inc.
All rights reserved. No part of this report may be reproduced or stored in a retrieval system
or transmitted in any form or by any means, without prior written permission.

EXECUTIVE SUMMARY

Conducting e-Business requires companies to address a new kind of risk as a part of their business strategy. Managing risk itself is not a new requirement; companies have routinely built risk-management models into their business plans. Historically, however, businesses have not adequately included their information assets in this modeling, and this practice must change. As a greater percentage of business transactions move online, a company's information assets have taken on greater importance with regard to business success and, at the same time, have become more vulnerable to attack than at any time in the past. This paper will address the new risks to which an e-Business is exposed, why those risks matter, and what can be done to manage them. Tivoli's SecureWay® Risk Manager product will be examined as an example of an enterprise risk management solution.

Why Risk Management?

Risk is inherent in conducting business. For as long as people have been transacting business with each other, the need has existed to assess and mitigate the risks incurred.

When neighbors bartered with each other, the risks inherent in the transaction — nonpayment, for example — may have been small enough that people were willing to take their business partner's word. Becoming known as a liar was a significant liability, and the value of an individual's word would have been widely known within that person's geographic trade area.

The brick-and-mortar world harbors significantly more potential risks to business success — risks to the completion of a transaction, such as nonpayment, late delivery, and outright fraud, as well as physical risks to operations, such as theft, arson, and even natural disasters such as earthquakes or floods. Numerous methods to understand, quantify, and limit these risks have been developed. Policies and procedures dictate requirements that must be met to transact business with a third party; financial and credit mechanisms ensure payment while mitigating the risk for both parties (the buyer doesn't have to hand over cash before receiving benefit, while the supplier has guaranteed payment); door locks, burglar alarms, and fire alarms combat physical risks; and the insurance industry exists purely because it is impossible to eliminate every risk entirely — insurance policies mitigate those risks which cannot be avoided.

As companies embrace e-Business, they are faced with a new and large set of risks. As a company's network has become a means to transact business, online threats have increased in number and severity.

A company's network infrastructure was once a private domain in which users were employees — generally employees who were inside the physical plant. Maintenance and security of the corporate network infrastructure were the responsibility of the IT department. When initial use of the Internet required companies to connect beyond the corporate office, security was viewed as a perimeter issue — firewalls controlled traffic into and out of the network, and the goal was to keep the bad guys out. This view worked as long as a company was using the Internet primarily for marketing — with an informational but not interactive web presence.

 For as long as people
 have been transacting
 business with each other,
 the need has existed
 to assess and mitigate
 the risks incurred.

The success of an e-Business depends not on its ability to keep the bad people out, but on its ability to give access to those with whom a company wants to do business, be they suppliers, partners, or new and unknown web surfers.

e-Business has turned this view of security upside down. By its nature, e-Business requires significant transactions to take place online — between companies and individuals with varying levels of trust and knowledge about each other. The success of an e-Business depends not on its ability to keep the bad people out, but on its ability to give access to those with whom a company wants to do business, be they suppliers, partners, or new and unknown web surfers.

To achieve this level of connectivity with current and potential partners and buyers, companies are opening their networks. With this increased openness, however, comes an entirely new set of business risks. A company's information assets have taken on an astonishingly new level of importance as business drivers,

and at the same time these assets have become more vulnerable to attack. It is harder to control who has access to which resources from a policy perspective, and threats such as hacking have become more prevalent. Viruses now spread through companies in minutes and through entire geographic areas in hours. And despite the public outages caused by last spring's denial of service attacks, most networks are as vulnerable today as they were then. Along with increasing external threats, employees are likely to have access to more information resources than in the past, opening up risks from both accidental misuse and intentional harm through theft or retaliation.

To complicate matters, companies are implementing sophisticated network architectures at a time when good IT talent is becoming harder to find, and when security practitioners are so scarce that experienced professionals can command salaries higher than their bosses'. This talent shortage often results in avoidable risks not being caught — servers being misconfigured, patches not being applied, and security policies and practices becoming reactionary rather than proactive.

As with previous business revolutions, eliminating risk is not possible (although some security vendors may try to tell you differently). What companies can and must do is understand, limit, and manage the risks involved in conducting e-Business. Managing the electronic risks that come with opening one's networks enables a company to manage its business risks. e-Business has created an environment in which a technical attack can translate directly into legal liability (if confidential

Eliminating risk is not possible. What companies can and must do is understand, limit, and manage the risks involved in conducting e-Business.

information is exposed), a drop in customer confidence (due to a downed site or exposed information), lost income, and even a loss of brand equity. Hacking is no longer an elite activity targeted at government networks. Companies of all types are finding themselves the target of electronic attack, often by amateurs armed with readily available tools, and a graffitied web site now warrants coverage by the national news outlets.

How to Manage Risk

To responsibly engage in e-Business, companies need to manage electronic risks as a part of their business model. To manage these risks, companies must:

- ▶ **Understand their risk.** Identify the areas that are vulnerable to electronic security breaches.
- ▶ **Limit exposures.** Architect the e-Business strategy to eliminate unnecessary exposure and risk.
- ▶ **Mitigate those risks.** Some risk is going to be unavoidable. Limit these risks through the implementation of security policies, best practices, and technologies.

 To responsibly engage
 in e-Business, companies
 need to manage
 electronic risks as a part
 of their business model.

The rest of this paper will focus on how to understand and address the risks that are unavoidable when implementing e-Business. Just as a company cannot eliminate the possibility that thieves may attempt to steal its equipment, a company also cannot eliminate the possibility that someone will try to break into or misuse its network and information assets. Similarly, just as the same company can install door locks and electronic surveillance systems, many steps can be taken to protect information resources as well. Understanding and implementing these risk mitigators is essential to any successful e-Business.

Security Products — Risk Mitigators

The security technology community has been working hard to address new threats to information security as each advance in e-Business creates new vulnerabilities. Many solid products exist today to provide protection against some of the threats described in the previous section. Firewalls continue to provide an important function at the network perimeter; intrusion detection systems can help administrators identify attempts to hack or overwhelm the system; access control products provide the ability to set fine-grained controls on what authenticated users can do and see on the network; and many other products, such as antivirus software, public key infrastructure (PKI), and virtual private networks (VPNs), exist to fill specific functions, from stopping virus infections to ensuring the privacy and integrity of electronic communications.

Most companies already use at least a reasonable subset of these products. Certainly an important step in limiting the risk to business is to understand which areas are vulnerable and to implement appropriate security technologies and products. Whereas companies with remote employees are likely to consider VPN technologies, companies pursuing high-value transactions online may need a PKI, and most e-Businesses will require firewalls, methods to detect and combat intrusion, protection against viruses, and access control.

This presents the question — if a company has analyzed its vulnerabilities and deployed appropriate security products, has it effectively mitigated its risk from online threats? The answer is no. A well-architected e-Security solution should be more than just a collection of these point products. Each of these products provides considerable value but only provides a view of a subset of the existing security threats. Because each product generally must be administered independently and provides alerts through its own console, security administrators cannot easily correlate alerts between products or catch patterns that occur over multiple security domains.

For example, an intrusion detection system (IDS) provides a view of traffic on the network geared at detecting unauthorized traffic and potential hacks. IDS products provide important information but are not in themselves enough to mitigate all of a company's e-Business risks. An IDS provides one view of network security, but many products have problems with false alarms — leading to a “boy who cried wolf” syndrome. To take full advantage of information gathered by the IDS, that information needs to be integrated with information from other security monitors. Similarly, firewalls are well suited to what they do, but they only address boundary level security, showing what's happening at the network perimeter, and any alarms they generate must be evaluated separately. The same is true for antivirus and other security products.

Many of these products can generate copious amounts of alerts and alarms. Since each point product implements only a subset of the overall security functions, these alerts trigger a large number of false positives. When network administrators are routinely faced with alarms resulting from normal behavior, they can become less worried and therefore less responsive when a real attack is occurring. What is needed for the best understanding of the true state of security at any point in time is a way to integrate and correlate the information gathered by each product. A real time, scalable method for correlating

What is needed for the best understanding of the true state of security at any point in time is a way to integrate and correlate the information gathered by each product.

and managing information gathered by multiple products is sorely needed to maximize the value of a well thought-out security architecture.

Although vendors are working toward supporting interoperability between products, at this point that is more of a goal than a reality. Furthermore, at most companies, security products have been implemented independently over time. Whereas the firewall may have been in place for years, the IDS system may have gone in last spring. To correlate reports manually would be both time-consuming and expensive, and although it might provide a better after-the-fact understanding of how an attack had occurred, it would eliminate the immediacy of the alert process, making the task useless for combating security threats as they occur. When there is no way to manage all these products from a central location, individual product vulnerabilities are often masked.

What Can Be Done About This?

To remedy this situation and maximize the effectiveness of its security defenses, companies need to provide a scalable event-management platform to integrate and manage security products and correlate the information they provide. Such a system would provide:

- ▶ **A centralized repository for event reporting and alerts from products such as firewalls, antivirus software, IDS, and web-server security.**
- ▶ **Correlation of the information received from multiple products.** This would provide the ability to “cross-check” alerts and would reduce the number of false positives that are generated.
- ▶ **One console to present alerts to administrators.** Correlated alerts should be presented in clear terms, while the individual events that triggered the alert should still be available for analysis.
- ▶ **Response capabilities that allow administrators to set policies to generate automatic responses triggered by security events.** This would enable immediate action in the event of a serious attack.
- ▶ **Proactive assessment and diagnosis of the state of individual products.**

An Example Solution — Tivoli SecureWay Risk Manager

Tivoli SecureWay Risk Manager is the result of Tivoli's attempt to define the requirements of enterprise risk management, and it provides an impressive set of capabilities (see Figure 1). Tivoli SecureWay Risk Manager runs on top of Tivoli Enterprise Console (TEC), enabling consolidated monitoring of and correlation of events from multiple products, a single console for presentation of correlated events, automated response options, and sophisticated analysis with multidimensional reports showing event history to pinpoint trouble spots and aid planning.

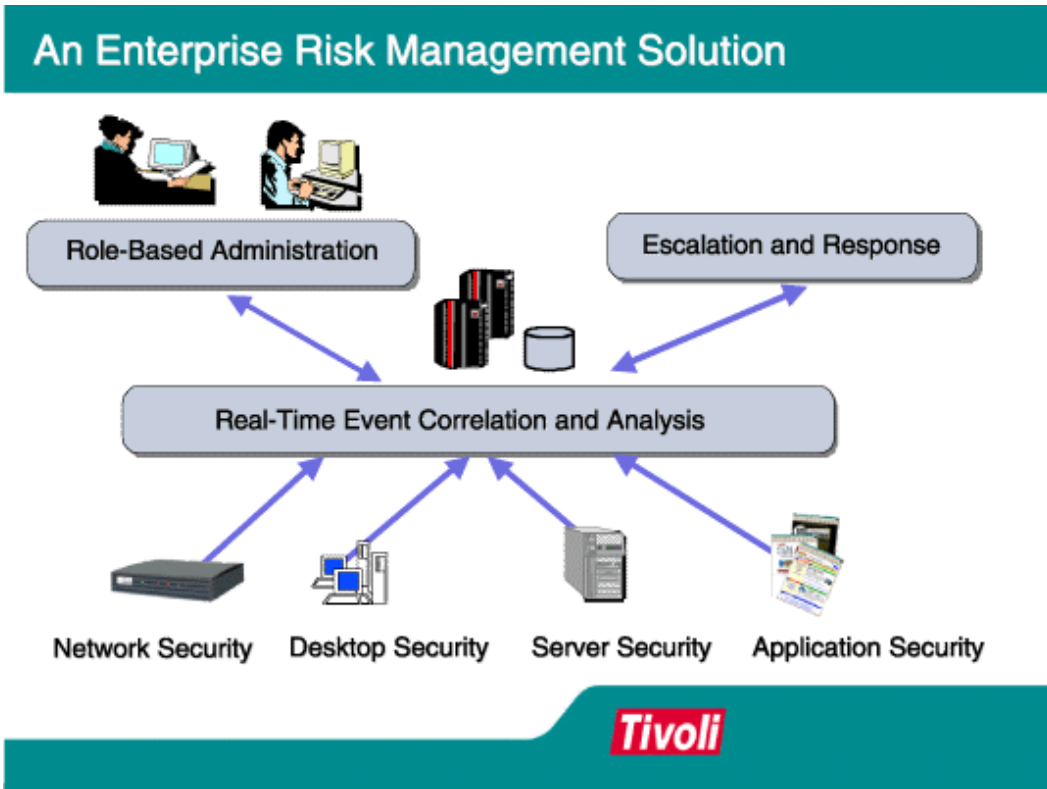


Figure 1. Tivoli SecureWay Risk Manager defines the requirements of enterprise risk management.

Although the first release of the product provided the required base engines for correlation and analysis, it provided limited product coverage, which limited the value that could be obtained with an out-of-the-box set up. In Tivoli SecureWay Risk Manager 3.7, Tivoli delivers on the promise of enterprise risk management, supporting the top products in each coverage area and providing for easy integration of additional products. A variety of security technology vendors are currently integrating their solutions with Tivoli SecureWay Risk Manager.

Products that are monitored and managed out-of-the-box:

- ▶ Firewall — Check Point Firewall-1, Cisco PIX Firewall
- ▶ Routers — Cisco
- ▶ Antivirus — Symantec Norton AntiVirus
- ▶ Intrusion detection systems — Cisco Secure IDS, ISS RealSecure Network Engine, ISS Real Secure System Agent, Tivoli Web Intrusion Detection System, and Tivoli Network Intrusion Detection System (available only with Tivoli SecureWay Risk Manager)
- ▶ Servers — AIX Servers, Sun Servers ,Windows Servers
- ▶ Application servers — IBM WebSphere, Lotus Domino
- ▶ Web servers — Microsoft IIS, Apache, Netscape Web Servers

Tivoli claims that because the work has been done to understand each “type” of input, other products of each type (such as a different antivirus software package) can be integrated in a few days.

Tivoli SecureWay Risk Manager’s cross-correlation of security events is designed to reduce false positives and provide administrators with an integrated view of what is happening on the network. Additionally, Tivoli SecureWay Risk Manager enables administrators to set up automated responses to specific attacks. Although automated responses do present the possibility that services could be shut down due to a false alarm, the correlation reduces this risk over individual point products. The decision of whether to automate responses will need to be made on a case-by-case basis, and the highest value will be achieved in automatically managing the types of events for which false positives are not an issue, such as removing viruses.

 Tivoli SecureWay Risk
 Manager’s cross-correlation
 of security events is designed
 to reduce false positives and
 provide administrators with
 an integrated view of what
 is happening on the network.

Integration with a variety of Tivoli and non-Tivoli enterprise systems management products enable the Tivoli SecureWay Risk Manager to recommend and enforce enterprise security policy improvements very easily (e.g., Security Administrator requests/enforces immediate deployment of a new Outlook patch to prevent further damages derived from the “I love you” virus). Tivoli has named this last capability “Decision Support for Enterprise Risk Management,” emphasizing the ability of the product to provide information to support security policy decisions in addition to event correlation and response capabilities.

The requirements for Tivoli SecureWay Risk Manager are lightweight and priced so as not to limit customers to Tivoli’s existing base. To prove this, Tivoli is working with security service providers on a program in which the service providers will install one or more Enterprise Risk Management services modules. With an Enterprise Risk Management service, customers get firewall management, intrusion detection and response, risk and vulnerability assessment, virus management, web security management, and router security management. All of these services are based on the combination of Tivoli SecureWay Risk Manager and integrated “best-of-breed” security technologies.

Conclusion

Businesses are facing continually increasing online threats to their networks. A large number of excellent point products address individual security functions. To better protect e-Business resources, however, companies need to ensure better management of their security products.

To better protect
e-Business resources,
companies need to ensure
better management
of their security products.

A system that can correlate alarms and information from multiple products provides a better view into the state of network security and a better ability to respond to threats. In Tivoli SecureWay Risk Manager, Tivoli provides centralized management of security products with an intelligent engine to improve responses to threats — be they hacking attempts or unauthorized access by employees — and analysis and reporting to enable better understanding of risks and provide a basis for improving the security architecture.

This much-needed functionality should enable companies to manage and mitigate the unavoidable risks of doing e-Business. Companies that are not already Tivoli customers may be wary of the prerequisite of TEC; however, Tivoli has structured the pricing so that this should not be a barrier.

Experience. Insight. Action.

Hurwitz Group, Inc. is a research and consulting firm providing strategic guidance with e-Business initiatives and is recognized for its real-world experience and pragmatic approach. Clients include Fortune 2000 organizations as well as business-to-business software and services vendors. Hurwitz Group strategists leverage the company's research to provide market development and positioning strategies, enterprise technology strategies, and custom consulting.