RedSiren White Paper

Security Wellness

A Holistic Approach to Protecting Your Enterprise's Assets

August 2001

RedSiren Technologies, Inc.
888-434-6734 or 412-281-4427
info@redsiren.com
www.redsiren.com

"Companies should consider trust services as a new cost of doing business in the information economy."

--"Creating the Trust Platform," Jupiter Media Metrix, 2001

Identifying the Need for Security Services

In the race to gain a competitive edge, companies across all industries are adopting e-business practices and implementing strategies designed to reduce costs and increase operational efficiencies. But at the same time, using the Internet or emerging networking technologies to centralize and improve business operations can put a company's security practices at risk.

The advent of federal regulations, including the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach Bliley Act (GLBA), is forcing companies in two of the nation's biggest industries—healthcare and financial services, respectively—to implement security measures to protect their customers' personal information. And it is widely acknowledged that most industries, including retail, manufacturing, distribution, travel and entertainment, will be affected by similar legislation by 2002.

What is Enterprise Risk?

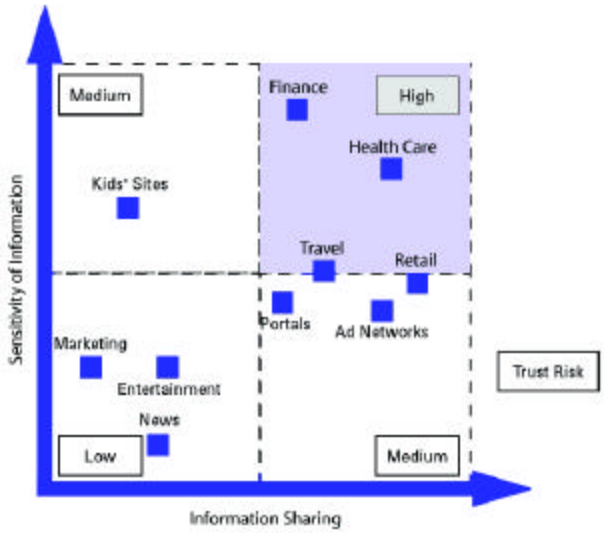
It's no secret that most Internet users have concerns about privacy. Frequently, Web site visitors must pass along "required" personal information such as names, addresses, birthdays or even social security numbers to just research price quotes or read articles. Simultaneously, Web-savvy customers who feel comfortable buying products and services online are demanding better customer service and 24x7 access to their account information. Either way, companies who rely on e-commerce to conduct business are exposing their customers—as well as their enterprises—to privacy and security risk.

As additional federal mandates concerning the collection of personal consumer data for marketing purposes come down the pike, companies must evaluate their enterprise risk, or how the potential for lost sales and increased infrastructure costs due to privacy and security issues could have a negative impact on their business. Unintended exposure of customer data leaves a company wide open for media attack, public scrutiny, lost profits—and legal action. The simple perception of a privacy or security breach is enough to create consumer mistrust and frenzy, as was the case recently when Microsoft® announced plans to use its Windows® XP operating system to collect user data, inducing the Electronic Privacy Information Center to file a complaint with the Federal Trade Commission.

New business processes, including the deployment of new technologies and the outsourcing of critical business practices such as human resources, also increase enterprise risk. For instance, CRM technologies are centralizing customer data, making it more accessible by a wider audience throughout the enterprise. As computers become increasingly networked, privacy and security threats multiply. A company's corporate network is only as strong as its weakest link; one minor, overlooked "hole" in the system could unexpectedly immobilize your entire corporate network or expose sensitive customer data. Earlier this year, for instance, the FBI began investigating more than 40 cases in 20 states where a gang of Russian and Eastern European cyber-criminals had been systematically exploiting Windows NT vulnerabilities. These criminals followed up with attempts to extort money from the victimized organizations. No matter what your operating system is, if your computers are connected to the Internet, then you are vulnerable to such attacks.

Security Wellness: Who's Watching Your Network?
Security experts warn that the recent "Code Red" pandemonium is just a symptom of future threats. In an Aug. 6, 2001 report, the *New York Times* cited security experts as saying that new viruses will "not only spread and operate automatically, but will target routers and larger components of networks." ***Any organization is a target for cyber-attack, regardless of size and reputation.*** During the first three quarters of 2000, over 15,000 computer attacks were reported to the Computer Emergency Response Team (CERT) at Carnegie Mellon University. In a separate study by the Computer Security Institute, 90 percent of the companies surveyed detected security breaches within the last 12 months. These numbers most likely are under-reported, considering that incidents of security compromises can often result in loss of customer and shareholder confidence, as well as company valuation.

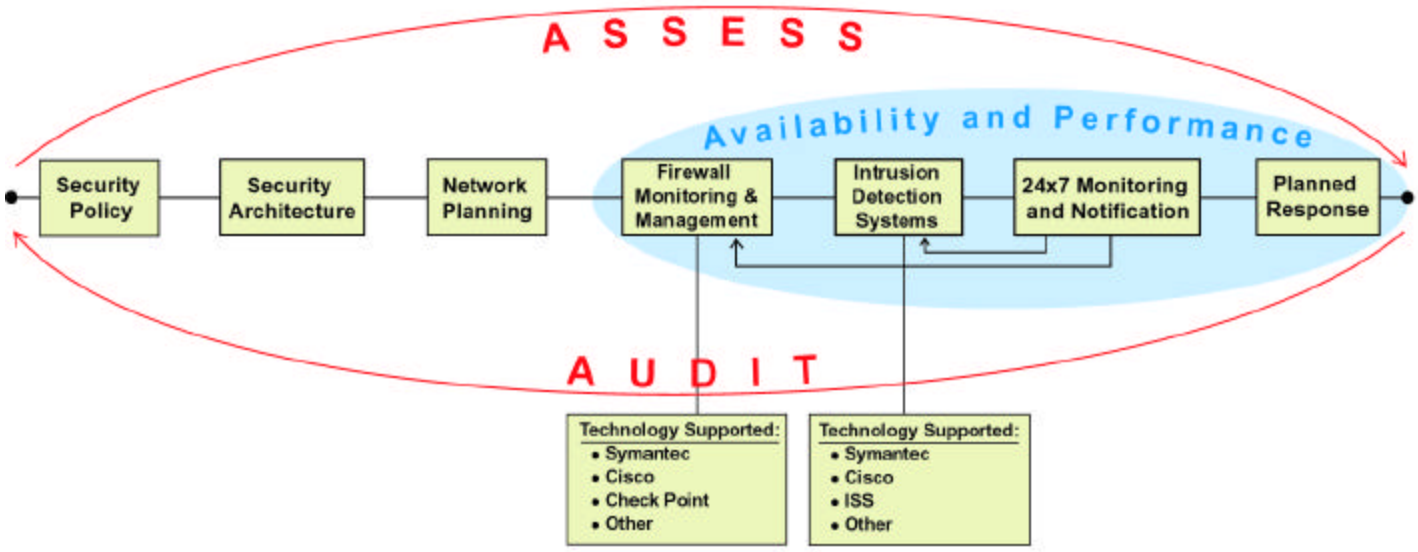
Enterprise Risk Across Vertical Industries



Just as a homeowner may protect his property by not only locking the doors but also by setting up an alarm system or installing motion lights, the availability and performance of a corporate network fundamentally is based on a system of protective "layers"—ones that prevent invaders from entering and, at the same time, limit residents' access to specific areas. This approach helps to protect a network by establishing a system of obstacles and safeguards.

RedSiren's approach is one of "security wellness." Security wellness focuses not just on one piece of the information security puzzle, but also on the 24x7x365 health of an enterprise's system and network as a whole. Security wellness is an ongoing, proactive and reactive relationship, not just a one-time solution. RedSiren's holistic solutions provide total system wellness by addressing ongoing security, performance and availability issues.

SECURITY WELLNESS CONTINUUM



RedSiren's Security Wellness Continuum focuses on the ongoing availability and performance of a corporate network through a system of 24x7x365 firewall management, intrusion detection services, and assessment recommendations.

It's a Matter of Policy

The foundation of any security wellness program is a security policy. As new government mandates come to fruition, having a defined, communicated and enforced security policy is increasingly important to the well being of your corporate network. All other components of security are derived from this overarching document.

To be effective, a security policy must have defined requirements:

- What are you trying to protect?
- Why are you trying to protect it?
- And from whom?
- Who will be in charge of protecting these assets?

A policy is a high-level document that provides guidelines for guarding the company's assets. It must incorporate a number of factors that have been signed and enforced by senior-level management, including:

- "Appropriate Use" statement regarding equipment use, company e-mail, Internet usage and passwords
- Firewall policy
- Disaster planning and recovery
- Incident response
- System assessment and auditing

In other words, if an employee asks, "What is the company's position on the use of e-mail?", the answers should be in the security policy in the form of specific procedures. For example, if a security policy states, "The IT staff will provide a means of recovery from a natural or man-made disaster within 24 hours," the policy must state how the IT staff will recover. Lastly, the security policy needs to take into account any given company's specific business—not only vertical markets, but a company's business needs—because security policies cannot be transferred cleanly from one company to another.

So You've Developed a Policy…Now What?

Once an enterprise has created a formal security policy, it needs to determine how the policy will be implemented. The first step in implementing the policy is to build the security infrastructure, which will determine how the policy will be fulfilled. For example, should a security policy state that employees must have access to e-mail and network files while on the road, the security architecture needs to create a remote access system that is integrated into the existing network.

This step is often challenging. Because of the dynamic nature of business, it is hard to plan for growth and anticipate the direction of the company in the next six months, let alone year two or three. To combat this, companies must treat a security program as an ongoing, living cycle, incorporating timely reviews of policies and rule sets.

Your First Line of Defense

As the first line of defense for a corporate network, a firewall must enforce the security policy. This means the firewall must be managed properly. The operating system and firewall application must be kept up-to-date to defend against the latest attacks. Also, the firewall's configuration must be protected. Immediate detection of activity aimed at comprising the integrity and configuration of the firewall is critical. As an early warning and prevention system, firewalls are important, but enforcement must be consistent and in accordance with the security policy. Unfortunately, the sole installation of a firewall may not be enough to detect or prevent a network intrusion, nor can it help a corporation respond to threats or react strategically should an attack occur.

"But…I Have a Firewall!"

While a firewall's filtering mechanisms help to prevent attacks, its intrinsic weaknesses make it vulnerable to probing and attack. After all, you can have a horde of 300-pound, 6'4" defensive tackles on your team, but if the opponent has a better offense, their players will undoubtedly find their way into your end zone. Taking into account a study from the Butler Group, which found that 80 percent of IT-related crime is committed by company insiders, simply installing a firewall is not enough to protect your data, ensure customer confidence and secure your assets. Disgruntled and dishonest employees, or a hacker who breaks down a firewall "for fun," can crumble a network without a moment's notice.

Intrusion detection services (IDS) are your next level of protection. IDS is the analysis of activity on a server or network. It is focused on discovering unauthorized or unwanted activity. Regarding RedSiren's unique wellness approach to security, IDS serves as a complement to perimeter security countermeasures. While a firewall prohibits certain types of traffic from entering your network, IDS is a safety net and catches intruders who sneak past the firewall.

A Hacker's Day Doesn't End at 5 p.m.

The majority of the business world operates between the hours of 8 a.m. and 6 p.m. Yet, hackers often are at their peak during off hours, when a company's IT resources are low. Just as most burglars thieve after nightfall or while the homeowners are away, a high percentage of intrusions occur after daylight employees have gone home for the day—when, more often than not, no one is watching the network.

A company's Internet connection is always on. Hackers are always on as well. If no one is there to hear the alarm, IDS provides a false sense of security.

Planned Response

Most people remember the shrill whistle of school fire drills. Although they were a welcome study break for the students, their singular purpose was to prepare the school in an emergency. In network security, preparing a planned response is mission critical should a contingency occur. In a crisis situation, each individual in the company needs to be prepared and armed with the tools to respond. The planned response should be designed during the network's planning phase. If an intrusion occurs, there will be no time to waffle about "what to do next." Normal operations must be quickly restored.

The most important component of a planned response is the empowerment of the Incident Response Team. During a crisis, the team will need to respond swiftly and follow pre-established procedures. When every second counts, pre-granted permission will save valuable time in reestablishing an operational system. Periodic drills, including “ethical hacks" should be conducted to make sure the plan is up to speed and accurate.

The Cyclical Nature of Security Wellness

The goal of security wellness is to put up multiple obstacles to slow or prevent an intruder from entering. To mitigate the risk of intrusion, a company needs to establish layers of security to offset individual component weaknesses. True security wellness is achieved when all of these modules fit together to lower a company's risk to an acceptable level.

Additionally, it is important to note that the Security Wellness Continuum is an ongoing cycle. Security policies, network architectures, firewall rules and intrusion detection signatures should be audited and assessed on a recurring basis to evolve with the growth of the company's infrastructure.

For example, a firewall assessment will determine if any vulnerabilities exist within the operating system or firewall application; what types of traffic are allowed to pass through; how the firewall interacts with Internet servers such as Web servers; and whether there is a need for redundancy on the firewall. An audit of a firewall will examine changes made to the configuration; whether the rules on the firewall support the security policy; and inspect the logs to determine if any violations have occurred. Both are critical and need to be conducted on a recurring basis.

To thoroughly minimize risk, a system of “checks and balances" concentrating on security audits twice a year, around-the-clock security monitoring and improved physical security is the key. A compliance review and "ethical hack" is also crucial to uncover any weaknesses and vulnerabilities.

How Can a Company Minimize Risk?

IT departments often find themselves swimming against the current when it comes to implementing security management programs. Although companies may realize the critical need of putting risk management plans in place, tightened budgets and limited resources are a common hindrance. In fact, according to the Meta Group, Inc., 50 percent of security positions are unfilled, and most CIOs became aware of the need for security only after a staffing shortage called attention to it. Yet, for companies transmitting their customers' highly sensitive personal data over a network, risk management is not just a "nice-to-have"—it is a priority.

Nevertheless, few companies have the required in-house expertise to develop and implement a strategic enterprise risk management program. It is also difficult for in-house staff to maintain timely information of liability and security advancements, or provide around-the-clock monitoring.

Without the tools, budget or staff in place to implement an internal, thorough risk management program, many companies are turning to managed security services providers (MSSP) like RedSiren. MSSPs offer a variety of products and services, including:

- Policy management, such as risk assessment and policy negotiation
- Risk management, including user administration, intrusion detection, security audits, and escalation
- Forensics, such as response, capture, and recovery of data
- Enforcement issues involving identity and permissions

Many companies are partnering with MSSPs for consulting and vulnerability assessments, policy reviews, virtual private networks (VPNs), intrusion detection services (IDS) and firewall monitoring. To achieve true "security wellness," corporations need to make sure their MSSP can provide a true continuum of services, from policy management to planned response should a breach occur. Moreover, MSSPs that can provide services without the need for additional investment in technology are advantageous in terms of minimizing IT infrastructure costs.

Experts indicate that by next year, security policy and security architecture development will become the foremost business issue due to customer demands for 24x7 operations support, as well as increased requirements for security experts with broader skills. Uncertainty about the status of a corporation's network security is surely a cause for concern. The old adage "no time like the present" certainly holds true in terms of network security, since not attending to security matters now could cost a corporation significant amounts of capital in the long run.

Security Wellness is an Insurance Policy
As corporations continue to tighten IT departmental budgets in response to the economic downturn, attention needs to be paid to the fact that risk management is a business issue; one that mandates thorough security and auditing practices. An investment in risk management, therefore, should be thought of as a long-term insurance policy, rather than as a return on investment.

As enterprises expand or become diversified, creating more user accounts and privileges to manage, the need for a standardized, controlled security system becomes imperative. Mergers and acquisitions are creating global Goliaths. As companies grow, mainframes and networks reproduce, forcing overworked IT staff to keep pace. It's true: there are no 100-percent security solutions. A partnership with an MSSP like RedSiren enables companies to protect network assets and remain compliant as more federal mandates are realized. It also can give corporations a competitive advantage in an e-business world by ensuring the protection and privacy of personal data, thereby strengthening customer loyalty and satisfaction.

How Can RedSiren Help?
As a leading managed security services provider, RedSiren is the single source for network and infrastructure availability, performance and security. Our team of CISSP security consultants and technicians deliver a comprehensive set of security-related services, including 24x7x365 remote security monitoring and management, remote perimeter management, as well as the security of application servers and critical devices throughout the corporate network.

RedSiren's Wellness Continuum provides a framework for establishing a security program in virtually any company or organization. By utilizing RedSiren's security services, our certified and trained security professionals can work with a company to establish an individualized security program.

In addition, RedSiren's on-site consulting offers customers a wide range of services, from definition of business requirements, security architecture and system design and security product integration, to on-site incident recovery services.

So How Do I Get Started?
RedSiren takes a multi-tiered methodology to help you assess and maintain the security of your environment. Understanding the company's current "state-of-security" in the context of your business goals is the first and essential step in defining or modifying a security policy. RedSiren applies a structured, non-disruptive, non-intrusive approach to identify and assess the internal and external threats and vulnerabilities to which your environment is exposed.

Our **Internet Vulnerability Assessment** (IVA) examines your company's network security from the outside. Our certified technicians perform an audit to identify the security posture of your "Internet-visible" infrastructure beyond your firewall. Using a variety of tools and techniques, we scan the vital assets that external Internet users and hackers can reach, such as firewalls and FTP servers, and analyze the results along with other site information. We combine our findings to give your organization a clear picture of the threats and vulnerabilities originating from external sources. Our report includes a detailed analysis and description of all conclusions along with a specific method to remedy any and all discoveries.

It is estimated that a high percentage of computer crimes occur from within an organization. Our **Corporate Vulnerability Assessment** (CVA), focuses on your company's network security from the inside. Our Security Specialists perform a thorough analysis of the overall security of your internal computing environment and its vulnerability to internal attack. Incorporating NIST, British Standards, and SEI's OCTAVE guidelines, RedSiren's experts use a combination of leading industry software tools and on-site interviews to analyze areas such as Security Policies, Physical Security, Access Control, User Awareness and Overall Vulnerability to an Internal Attack. Our team of specialists prepares a detailed analysis at a key asset level, outlining the detected vulnerabilities, the organizational impact and the steps that can be taken to mitigate risk.

For more information about RedSiren's security services, please visit http://www.redsiren.com.

RedSiren Technologies, Inc.
Centre City Tower
650 Smithfield Street
Pittsburgh, PA 15222
412-281-4427
888-434-6734
info@redsiren.com
www.redsiren.com