netForensics

Maximizing the Value of Security Information and Infrastructure

Growing concern over IT security's Return-On-Investment
is forcing web security to take a seat in the boardroom

A netForensics Whitepaper

Maximizing the Value of Security Information and Infrastructure

Growing concern over IT security's Return-On-Investment
is forcing web security to take a seat in the boardroom

IT Security awareness is rapidly gaining mind share and management increasingly understands the need to act quickly and wisely if they are to protect valuable corporate assets. Today's volatile cyber environment, combined with the complexities of building a security infrastructure, require the implementation of a complete, yet cost efficient, security strategy. The financial implications of security and the significant investment required to create an effective security system make it essential that management become more informed, involved and prepared.

Every day, companies make substantial investments in Internet security without knowing if the integrity of their business remains intact. In the past, security decisions were primarily based on technology and delegated to individuals with relevant technical expertise. Today, however, because of the financial implications of security and the significant investment required to create and maintain an effective security system, corporate management at the highest levels has become more involved in security strategy and its implementation. As a result, security infrastructure and security policy have become a vital part of the business plan, and gained an important seat in the boardroom. Security, therefore, has moved from being a luxury to a necessity.

Budgets for network security have increased dramatically in the last year alone, as spending has rapidly increased across all industry sectors. The Gartner Group reports that IT security funding has increased to as much as 8 percent, up from approximately 3 percent of total budgets a year ago. According to *Information Security* magazine, the number of companies with annual security budgets of more than $1 million has doubled from 1999-2000 and increased 188% since 1998 – mostly in banking, financial services and high tech.

As companies spend more on security, however, they have not necessarily made themselves more secure. Despite a marked increase in security spending, cyber attacks continue to proliferate. t appears that increases in security IT spending have not matched the explosive growth of cyber attacks – the hacker community is usually able to devise new attacks faster than the security industry can respond. As a result, businesses have reacted to growing intrusion attacks by installing scores of firewalls as their primary defensive strategy. Only now are companies beginning to proactively create effective and complete security strategies with specific policies and response procedures. They have built detection systems and Virtual Private Networks (VPNs). They even run periodic vulnerability assessments to identify holes in their systems.

Essential Questions That Guide Risk Management

As companies are dedicating more dollars to security hardware and software, upper management is starting to ask questions to assist in formulating risk management strategies:

- Who is attacking our resources?

- Did the attack originate from inside or outside the organization?
- How are they gaining access to our network?
- How do we know if our security point solutions are working?
- Which systems and applications are being targeted or attacked?
- What is happening when an attacker gets in?
- What is the impact of these attacks?
- When have these attacks occurred? Is there a pattern?
- Why are particular systems being targeted?
- How can attacks and intrusion be prevented?
- Who is notified of an attack and are they qualified to respond to the threat?

The answers to these questions lie in the vast quantities of valuable information generated by the installed base of the security infrastructure. However, reams of critical data are often neglected, ignored and even discarded by an already overworked IT staff that has little time to analyze the information. Budget constraints also limit the labor hours available to manually monitor these devices. Further, the lack of qualified and trained personnel in the IT labor force makes it virtually impossible to properly manage security information without automation.

Security Information Management (SIM) Addresses Critical Issues

In today's volatile cyber-environment, management needs continuous information and analysis on the events occurring within the security infrastructure so that business exposure and threats may be minimized and potentially costly liabilities avoided.

SIM focuses on providing:

- valuable information to support operations, security, engineering and auditing.
- continuous real-time information, notification and advanced analysis of high-data volume security infrastructure components.
- browser-based management that allows maximum scalability, consistency of deployment and low total cost of ownership.
- timely, consolidated reporting tools necessary to assure business management that their security investment is providing intended value.
- integration with multi-vendor security devices and applications to provide comprehensive analysis and alerting.

SIM ROI: Maximizing The Value of Security Information and Infrastructure

Management requires documented, clear evidence that their security investment is working as planned. They need to ensure that they are maximizing the value of all available information and resources. When developing and refining a security strategy, a crucial objective is to maximize the return on the investment that has already been made in security infrastructure point solutions; firewalls, intrusion detection systems, VPN, applications and host integrity systems. SIM enables enterprises to accomplish this by empowering the organization to:

- avoid the costs associated with a hack.
- reduce costs by improving resource allocation and increasing efficiencies.
- improve decision-making processes and speed response time.

Avoiding the Costs of a Hack

The Computer Security Institute (CSI) polled 643 computer security professionals. Ninety percent of the respondents found computer breaches in the last 12 months. Seventy-four percent of respondents acknowledged a financial loss. Another CSI study published earlier this year, in which 186 companies took part, found that the average loss to computer crime was $2 million per company. These losses centered around the following issues:

Loss of Revenue Due to Downtime – Industry experts employ statistical models to estimate downtime costs. Using conservative numbers, here is an example of costs associated with a security breach that results in a network outage:

Annual Company Revenue:	$ 25,000,000
Resulting Downtime:	4 Hours
Average Employee Salary (including benefits):	$ 80,000
Number of users effected by the Downtime:	100

The business impact costs for this same company are as follows:

Cost of Employee Downtime:	$ 15,385
Cost of Lost Business Revenue:	$ 48,007
Total Downtime Cost per occurrence:	$ 63,462

The CSI reports that computer viruses were the most common threat, costing companies an average of $61,729 last year. Denial of Service attacks cost an average of $108,717. The total annual loss last year for all forms of security breaches was over $15 billion, according to Datamonitor.

Taking into consideration that e-Business continues to emerge as a way to conduct business, it can be said that a network outage could seriously increase the associated business losses over what is stated here. If downtime increased to a day, if an e-Business website was severely breached and transactions lost or content destroyed, the associated losses would be greater. What about lost transaction data? Can that ever be recovered?

Litigation Costs – Companies that neglect to show due diligence in minimizing their exposure to cyber-threats are opening themselves up to extensive liabilities. There is not only an obligation of companies to install firewalls and other security point solutions, but to also have the methods in place to continuously control and monitor security information and the risks associated with e-commerce. Emerging privacy and security regulations include the Health Insurance Portability and Accountability Act (HIPPA) and the Gramm-Leach-Bliley Act (GLBA), which establishes specific security and privacy requirements for the financial industry. It is inevitable that other industries, educational institutions and government itself will be required to protect themselves and others from liabilities by adopting methods to effectively monitor and manage security information.

Cleaning up and restoring a hacked network – Post-hack consultants and evidence gatherers utilizing decompliers, data recovery programs and other forensics tools command fees often surpassing $20,000 per computer, according to recent study at the University of Washington.

Defensive remedies are expensive - When a security breach is experienced, companies must scramble to find a quick solution, usually an expensive approach to dealing with the problem. This can have a dramatic increase on the bottom line in the short-term.

Additional costs associated with being hacked:

- Damage to image and reputation
- Lack of customer confidence
- Loss of data, research, bids and other proprietary information
- Bankruptcy

Additional costs associated with avoiding a hack:

- Additional staff to monitor growing security infrastructures
- Being “pigeon-holed” into purchasing proprietary solutions

Reducing Costs to Gain Rapid ROI

There are vast quantities of critical information generated by the installed base of the security infrastructure. Security devices generate reams of critical data that is often neglected, ignored and even discarded by an already overworked IT staff. Particularly in today’s environment, budget constraints limit the labor hours available to manually monitor these devices. The lack of qualified and trained personnel make it virtually impossible to properly manage security information without an automated solution.

An effective SIM solution affords a rapid return on IT security investments by:

- reducing the cost of labor that is required to manually monitor security information.
- improving the utilization of security infrastructure; components, point solutions, traffic flows, volume and bandwidth.
- simplifying network tuning for higher performance.
- increasing efficiency as personnel previously used for monitoring security information can now dedicate time to other projects.

A new kind of ROI – 'Return On Information'

While traditional Return on Investment calculations focus on defining cost savings and the breakeven points of investments, there is no one-size-fits-all method of calculating SIM ROI. Alternative metrics should be employed to identify the qualitative advantages gained by instituting a particular security management solution. This analysis can be combined with hard numbers, such as those derived from cost savings, cost avoidance and revenue stream calculations. A multitude of designer ROI approaches are popping up, attempting to provide these metrics, and we are seeing the strong emergence of a new kind of ROI called Return On Information.

A Return on Information analysis focuses on the vital issues that comprise SIM and the benefits it provides in planning, scaling and executing IT security programs. What is the additional cost of this security information awareness above and beyond the investment that enterprise has already made in point solutions? Is your network industrial strength? What is the value of being able to react and respond to security events as they occur?

netForensics: Positioned at the Security Information Management Forefront

Many organizations have attempted to design their own programs to correlate and analyze security information, but in most cases, the expertise, time and resources do not exist in-house. The more experience technical professionals have in dealing with the complex problems associated with their networks and applications, the more likely they are to realize that a third party solution is required.

Another obstacle in implementing effective SIM has been the lack of standards in the security industry. The J.P. Morgan 2001 Security Update stated that, "The problem with many solutions now being brought to market is that when a major vendor offers a management solution, it is best suited to manage its own security products, but falls short in managing competing products. There is no standardization and no motivation for the vendors to work together. An independent management solution, such as netForensics, focuses specifically on the overall management layer."

netForensics Security Information Management is a comprehensive solution that efficiently manages security infrastructure resources and delivers a unique set of benefits:

- **Universal Correlation** provides the ability to see activity on different devices and applications at the same time and, therefore, be able to draw relationships based on this information. Security information is consolidated and visually correlated to help facilitate rapid analysis and decision-making.

- **Distributed Architecture** offers full, efficient scalability. Using innovative ActiveEnvoy™ Technology, netForensics enables security information to be collected, communicated and analyzed using secure XML/TCP and a *Universal Agent* protocol for rapid customized device and application integration.

- **Event Aggregation and Robust Filtering** provides rule-based data reduction from security devices and applications, maximizing performance and storage. Multiple levels of

filtering and event destination management reduce false-positives to focus on high-risk threats.

- **Scoring** enables the identification of potential threats from multiple low-level security events. netForensics identifies patterns of multiple, low severity attacks that may amount to a high severity attack by applying a repeating event score that is tracked and aggregated. This aggregated score is identified as a higher potential threat being masked by the intruder, effectively putting low-level events in context and raising the severity.

- **Web-Enabled Security Operations** allow global access, analysis and response to security events from any Java-enabled browser.

Today's Internet security systems, although sophisticated in their design and implementation, have been lacking one vital element; a reliable, online means to monitor and report their ongoing status and effectiveness. The missing link is now available with Security Information Management from netForensics, unequalled in its ability to provide timely, effective analysis, monitoring and reporting. Clearly, there is a new set of values in security monitoring driven by economics, technology and, most importantly, ROI.

For additional information and an online demo visit www.netforensics.com
or email sales@netforensics.com.

US Headquarters:

netForensics.com, Inc.
200 Metroplex Drive
Edison, NJ 08817
Tel: (732) 393-6000
Fax: (732) 393-6090

US Regional Sales Offices:

New England:	Walpole, MA	(508) 660-0336
Southwest:	Addison, TX	(972) 239-9777
Southeast:	Tampa, FL	(813) 361-8412
Midwest:	Chicago, IL	(312) 282-6493
Mid-Atlantic:	Philadelphia, PA	(215) 859-8288
West Coast:	Beaverton, OR	(503) 968-2270

International Sales:

info@netforensics.com