

Security Risk Management:

**Security Strategies for Managing Vulnerabilities and
Threats to Critical Digital Assets**

CRA Reports

*This report was prepared by
the Washington Bureau of
CRA Reports, an independent
editorial firm based in
Washington, DC.*

Copyright © 2003
All rights reserved

**Security Risk Management:
Strategies for Managing Vulnerabilities and
Threats to Critical Digital Assets**

Part 1. Introduction/Market Overview 3

Part 2. Operational Impact Analysis..... 7

Part 3. Technical Impact Analysis..... 10

Part 4. Cost/Benefit Analysis..... 12

Part 5. About the Sponsor: Foundstone..... 13

Editorial Director
Lane F. Cooper

Research Associate
Allison Johnson

PART 1:

**Security Risk Management:
Strategies for Managing Vulnerabilities and
Threats to Critical Digital Assets**

This White Paper explores the market trends that are creating requirements for Security Risk Management (SRM) strategies. It demonstrates how a multi-disciplinary approach to SRM can be most effectively integrated into the operations of companies. It describes the technological requirements for implementing an SRM strategy to protect critical information resources from events that can degrade or destroy strategic digital assets. Finally it provides a cost-benefit context against which SRM investments can be understood.

Nobody in corporate America denies the strategic imperatives associated with protecting the information infrastructures and data that underpin virtually all commercial activities in today's economy. And yet, despite the documented costs of cyber attacks by hackers, viruses – even trusted employees within organizations – the security posture in most large enterprises is still characterized by a series of largely disconnected measures and countermeasures designed to respond to events after they have occurred. Current security strategies are, in other words, reactive in nature – not proactive.

The management of enterprise digital asset risk across most sectors of corporate America has been delegated to technical teams and vendors whose operations have been bolted on to existing processes rather than integrated into the workflow that brings products and services to market. The executive attention that has enabled many organizations to achieve quantum leaps in efficiency from supply chain and customer relationship operations has not been brought to bear on the management of risk to the infrastructures that enable these same strategic enterprise initiatives.

It is the contention of this report that a strategic commitment to Security Risk Management is the only way to bring about significant improvements in the security posture of companies who rely increasingly on their computer and communications networks to do business. But it will require executives in these companies to not just provide oversight, but leadership in setting a tangible and measurably better risk management strategy that addresses security, disaster recovery and business continuity in a proactive, rather than reactive manner.

...Security Risk Management Defined

Security Risk Management, or SRM, is the systematic analysis of how various elements of risk affect corporate digital assets that allow organizations to identify, prioritize and mitigate risk in a rational manner. In order to implement an SRM strategy, it is necessary to understand the basic elements of risk. For the purposes of this report risk is defined by the following equation:

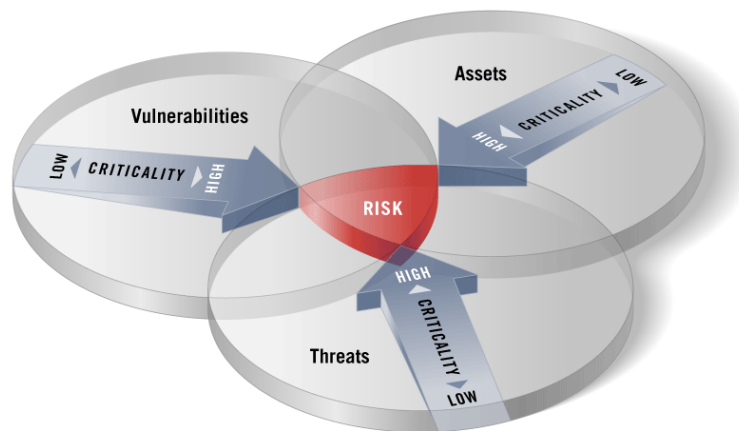
$$\text{Risk} = \text{Asset Value} \times \text{Vulnerability} \times \text{Threat}$$

The terms “vulnerability” and “threat” are often used as synonyms for “risk” by non-technical managers and executives. This explains the tactical – or point-solution-based – approach to security adopted by large segments of industry.

However, in order to strategically manage risk, it is important to have a clear idea of:

- Which information assets are critical to company operations;
- The extent to which critical assets are vulnerable to attack; and
- The nature of actual threats – active efforts – to access, corrupt and/or otherwise disrupt digital assets.

Understanding the interplay among these three variables provides the basis for making decisions about how to best mitigate and respond to risks companies face on a day-to-day basis. It represents a fundamental departure from the traditional standard operating procedures of most security organizations.



...The Status Quo: High Activity, Low Visibility/Accountability

The security teams in the overwhelming majority of companies in the United States are arguably the busiest knowledge-workers in the economy. The reason? Over a decade of fundamental change in the nature of corporate computer security operations has created a volume of threats unimaginable to experts in 1989.

- By 1990 computer and communication specialists started laying the groundwork for migrating large monolithic mainframe platforms to the client-server architectures that even then promised to democratize the use of IT resources within organizations. The migration introduced a new level of complexity in the management of computer security, as the number of people who could directly access corporate information systems leaped from the handful of specialist who filtered information requests to the mainframe, to a much larger number of line-of-business employees throughout the organization who could now download data and access applications at will. The amount of data that needed to be tracked to manage security and enterprise system risk rose accordingly.

- By 2000 another major migration – this time from client-server computing to web-based (N-tier) architectures – took place to support extended enterprise operations. The move again exploded the number of people requiring access to network resources. In fact, it created new classes of enterprise system users, as emerging business imperatives called for customers, suppliers and other go-to-market partners to access enterprise computing resources.
- The commercialization and industrialization of the Internet as the inter-corporate networking infrastructure, further exposed enterprise systems to new vulnerabilities and increased the number and types of threats that could attack, degrade and/or disable enterprise system operations. Between the creation of new access points for mobile employees, and the accommodation of new employees that have come in through corporate mergers and acquisitions, the number and nature of access points that security policies must address has grown tremendously.

Corporate America's primary strategy for dealing with the increased risk was to collect information about the gathering threats and create a layered set of countermeasures designed to respond to incidents that threatened enterprise resources.

Most businesses have concentrated their security efforts at the network perimeter, by way of authentication policies and firewall solutions designed to detect and reject unauthorized users and viruses.

Perimeter defenses remain an important element of security planning. But it is now equally clear to organizations in all industries that they need to police not just the borders, but also the people, pipelines and repositories that make up the entire enterprise system. Point solutions have arisen to address many of these vulnerabilities. But despite all of these measures, breaches occur.

- Documented financial losses from a survey of 530 respondents conducted this year by the Federal Bureau of Investigation (FBI) and the Computer Security Institute (CSI) totaled nearly \$202 million.
- And yet, this number does not provide a full accounting of the losses. For while a full 75 percent of organizations acknowledged financial loss, only 47percent could quantify them.

The volume of attacks detected by sensors and security countermeasures – including Intrusion Detection Systems (IDS), virus and firewall systems – has created a deluge of information to which corporate security teams must respond. As a result, the “information security war rooms” of many organizations are engaged in a constant fire drill as they address hundreds, perhaps even thousands, of daily alarms – many of which turn out to be false positives.

This event-driven approach to security allocates resources to threats on more or less a first-come-first-served basis – often without regard to the level of risk that a particular attack poses to the enterprise.

This reactive security posture recently prompted analysts at Stamford Conn.-based Gartner to issue a highly critical report of enterprise security paradigms that revolve primarily around responding to IDS-type alarms.

...Government Mandates for More Strategic Security

For a growing number of companies, emerging government regulations at the federal, state and local levels are further prompting a more strategic approach to managing risk. For instance:

- **Gramm-Leach-Bliley Act** – states that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
- **California's SB 1386** – a sweeping measure that mandates public disclosure of computer-security breaches in which confidential information of any California resident may have been compromised.
- **The Health Insurance Portability and Accountability Act** – will have a major impact on health care providers who do business electronically as well as many of their health care business partners. Many changes involve complex computer system modifications. Providers need to know how to make their practices compliant with HIPAA.
- **Sarbanes-Oxley Act** – is considered by many to be the single most important piece of legislation affecting corporate governance, financial disclosure and the practice of public accounting since the US securities laws of the early 1930s.
- **ISO 17799** – is an international standard based on BS7799. It is an international standard that requires risk management processes, procedures and tools for information security. Almost all of Europe has adopted this as a mandate for better computer security.
- **Common Criteria** – is also an international standard that is currently mandating consideration of security and vulnerabilities within the systems that are procured. The United States Government has already begun requiring the inclusion of protection profiles and evaluated software in all government environments.

“These regulations and laws have raised the ante on how companies treat security. Corporate management can’t simply delegate security responsibilities to the IT department without some kind of oversight. Moreover, threats are growing faster than companies can deploy point solutions to address them. So organizations need a much more coherent process. Otherwise they can spend a whole lot of money on security, and still not see the enterprise’s true security posture. This is increasingly unacceptable, as senior executives are held responsible for protecting and preserving the integrity of their information assets.” – Charles Kolodgy Analyst, IDC

Part 2:

Operational Impact Analysis

From an operational standpoint, the introduction of SRM into security operations provides an organizing principle around which a multi-disciplinary team of IT, security and line-of-business executives can “manage” the risk factors an organization faces on a day-to-day basis.

It elevates security from an arcane activity that responds to specific incidents, and provides a basis from which a more proactive strategy can be implemented to make certain that critical assets, applications and processes receive security resources that are commensurate with their importance to the organization.

“SRM leads to the creation of an effective execution plan that allows organizations to mitigate risk where it matters most first. It allows managers to focus their resources – knowledgeable IT and security teams and their tools – on areas that will have the highest impact on the organization. This way, fewer people and organizational resources can protect a higher proportion of assets that are truly important to the organization.” – Stuart McClure, CTO/President Foundstone, Inc.

...10 Step SRM Implementation Process

There are 10 basic elements to an SRM strategy that must be implemented to cover the entire security life cycle. Each discrete step plays a critical role in developing a proactive approach to security that cuts through the noise of tactical alarms, so that organizations can focus their response on events that can cause catastrophic harm. Each step reinforces the others, and the entire process should be seen as dynamic – rather than static – in nature.

1. **Establish an SRM Team** – Because SRM involves the evaluation of assets – as well as threats, vulnerabilities and security countermeasures – organizations that implement effective security initiatives must start by fielding a team of managers that can establish a comprehensive strategic security policy. The team should consist of line-of-business, corporate communications, legal, IT and security professionals.
2. **Develop a Comprehensive Security Policy** – Processes, standards and guidelines must be developed, disseminated and vetted to make certain the policies make business sense, and that there is enterprise-wide buy-in necessary to ensure comprehensive compliance.
3. **Take Inventory of all Digital Assets** – The policy must be based on a comprehensive inventory of assets that reside on the entire network – including shared network resources, such as those used to support inter-corporate operations like supply chain management. A rigorous and comprehensive survey must be conducted of all applications, databases, and processes that are enabled by the enterprise network.

4. **Prioritize Digital Assets** – This critical step in the process must be led by the line-of-business members of the SRM team. The process of assigning relative value to assets on the network can often be contentious – but it is also illuminating. It is an exercise that can help the entire organization focus – even rediscover – where core competencies lie, and what the most critical assets to the organization are. This process often reveals that inordinate amounts of resources have been allocated to protect resources that are of secondary importance to the organization. Given the realities of scarce resources, this means that more important assets received short shrift in the security process.
5. **Assess Vulnerabilities** – Determine the vulnerabilities that are present on the enterprise network, and determine how exposed those vulnerabilities – such as router mis-configurations, or missing database patches – are to threats. This process should include the assessment of access points and paths, as well as vulnerability chains – situations in which security breaches create new un-anticipated vulnerabilities.
6. **Threat Assessment** – Establish the extent to which hackers, viruses or even internal sources have probed (or continue to probe) the enterprise system for weaknesses.
7. **Determine Risk Score** – Create a system for determining risk based on:
 - The value of assets;
 - The extent to which elements of the enterprise system are vulnerable; and
 - The intensity of actual threats to those elements.(The scoring system should automatically attach high scores to high-value assets on vulnerable systems that appear to be exposed to active threats.)
8. **Establish Remediation Protocols** – Develop protocols and processes that prioritize enterprise system fixes based on the Risk Score.
9. **Monitor, Measure and Modify SRM** – Like any strategic enterprise initiative, SRM should be seen as an important ongoing process – not a tactical event. The impact of the entire system on both the security posture of the organization, as well as on the use of security and technical resources should be watched closely with an eye for finding areas of improvement.
10. **Enforce Compliance** – The SRM security policy must be taken seriously by the entire enterprise. If compliance with SRM policies places an onerous burden on operations, then steps should be taken to amend the policy. But there should be no exception to compliance. Senior executive commitment to the SRM team and the policy is critical to ensuring compliance.

...Operational Outcomes from Effective SRM

The most dramatic result from a successful SRM implementation will be the restoration of normalcy to the “information security war room.” The ability to identify areas of weakness (or high risk) proactively, rather than reactively responding to a flurry of alarms, should eliminate the fire-drill atmosphere that can develop every time a minor

event manifests itself. A rational SRM strategy allows organizations to establish reasonable risk tolerance levels and manage their response accordingly. It should allow organizations to establish a manageable policy based on the quality of assets that must be protected, allocating appropriate resources based on a solid understanding of the organization's risk level.

Part 3:

Technical Impact Analysis

Effectively implemented SRM strategies harness a broad set of technologies to capture data about threats and vulnerabilities associated with all elements of the enterprise network. It then presents managers with a single, understandable and actionable picture of the organization's risk posture. This is the only way that SRM teams can address challenges to the enterprise system in a proactive, integrated and automated manner.

...Specific Technological Requirements

Since most Fortune 1000 companies are moving toward a "web services" environment to manage emerging and existing technology assets, it makes sense for the SRM initiative to use the web as the platform from which risk can be assessed and managed. To that end, the following categories of technology should be integrated to field an effective SRM solution:

- **SRM Web Portal** – This should be the "cockpit" from which security policies are developed, executed, managed and monitored. All major SRM operations – from asset discovery and prioritization, to monitoring, remediation and reporting – should be controlled from this portal.
- **SRM Dashboard** – Risk status data should be presented in ways that are useful to the different types of players who work with SRM information (i.e. IT, security and line-of-business professionals). It is, consequently, critical to develop a "dashboard" that presents information in meaningful ways, and that provides appropriate context so that effective decisions can be made.
- **SRM Knowledge Management** – Given the dynamic nature of SRM – both threats and assets are constantly evolving in ways that affect the organization's risk posture – it is important to establish a repository of information that can help executives understand the constantly changing security picture.
- **Server and Application Inventory Management** – You can't manage what you don't measure. And you can't measure what you don't know. That is why it is important – especially for organizations with extended enterprise operations – to identify and analyze the contents of servers and establish the various types of applications that are on the enterprise system.
- **Authentication Management** – To mitigate the threat of "social engineering" and ensure that users are complying with security policies, systems should be put in place to make sure appropriate authentication measures are being taken prior to providing access to enterprise network resources.
- **Scanning Technology Management** – A great deal of thought should be put into selecting the core technology that is used to identify assets and vulnerabilities. For large organizations that are implementing a centralized strategic SRM initiative, it is critical that the scanning activities accommodate the distributed characteristics of the enterprise system.

- **Proactive Remediation Management** – As the SRM process transitions from analysis to action, there should be a direct relationship between information gathered on the organization’s risk posture, and the actions taken by the organization to address challenges to enterprise systems. All too often there is a “disconnect” between analysis and remediation. In other words, the status of remediation efforts should be visible on the same dashboard that reports the Risk Score of the various parts of an enterprise system.
- **Threat Correlation Management** – Organizations should constantly have their finger on the pulse of emerging threats to enterprise systems, and develop the ability to determine how those threats can potentially affect the organization. By correlating emerging threats with enterprise system vulnerabilities in an integrated manner, organizations can take proactive action and mitigate risk before an actual event takes place.

...Keeping the Risk Picture in Focus

Beyond the technology management issues identified above, the SRM team should look for ways to use any information source that can help keep the risk posture of the organization in focus. The challenge lies in making sure that the addition of new information does not overwhelm the decision makers managing the security policy.

Generally speaking, the objective of SRM-related initiatives is to develop filters that can put new stimuli into an understandable context. Rather than presenting SRM managers with raw data, the analytical capabilities of SRM should use the data to contribute to the risk score of any given element in an organization’s enterprise system.

Part 4:

Cost/Benefit Analysis

Unlike enterprise-wide initiatives that are designed to generate sales (such as CRM) or iron out costs (like SCM) security can be tricky to cost-justify. Determining return on investment in this case is a function of keeping potential actions from manifesting themselves. The impact of security events (such as denial of service attacks) will affect companies differently depending on the business models adopted and industries served.

E-commerce organizations and financial service organizations, for instance, stand to lose a great deal more from events that prevent customers from accessing web-based services, than professional services organizations who primarily use their web presence to advertise their offerings.

However, in virtually every instance, large enterprises can gain significant and measurable improvements from strategically implementing SRM – rather than continuing to support reactive information security tactics.

...What You Don't Know Can Hurt...A Lot

The inability to correlate threats with enterprise system vulnerabilities and asset value can have disastrous consequences. While it is easy to succumb to the illusion of awareness created by reports of breaches or attempts to access enterprise resources – in a fundamental business sense, the risk is being managed in a blind environment.

The reception of technical reports should not be confused with business intelligence. The fact that that on any given day an organization's security team responds to 80 percent of reported incidents (a generous stipulation) does not provide executives with meaningful insight into risk posture. A reactive approach to security – no matter how busy and conscientious the security team – cannot guarantee that the 20 percent of events that remain unaddressed are not wreaking havoc on mission critical digital assets.

...Allocating Resources Rationally

The flip side of the above point is that without some sort of an SRM strategy, organizations cannot allocate security resources (human resources, technology tools, and project funding) effectively and efficiently. A tactical approach to security means that events external to the organization dictate how resources are spent. And those events usually do not have the organization's best interest at heart. In fact, it is quite common for professional hackers to initiate a series of events with the objective of camouflaging their actual intent. It is the equivalent of starting a dumpster fire behind a grocery store, to deflect attention from a bank robbery on the other side of the neighborhood.

By using the risk scoring elements of an SRM strategy, it is possible for business decision makers to keep appropriate resources focused on mission-critical assets. Besides preventing the security team from being distracted by non-critical events, it enables the organization to actually maintain an improved Risk Posture with fewer resources.

Part 5:

About the Sponsor: Foundstone

Mission Viejo, California-based Foundstone has developed Enterprise Risk Solutions™ (ERS) that are designed to help Fortune 1000 companies discover, inventory and prioritize global network assets. The suite of offerings included in ERS provide organizations implementing SRM strategies with an integrated set of technologies that identify vulnerabilities and threats to mission-critical assets, providing continuous and proactive protection and intelligent, measurable remediation.

Foundstone's ERS enables clients to continuously monitor, respond to, and adjust to a changing risk environment. The company can rapidly map an entire global network, including wireless connections, while simultaneously probing for vulnerabilities. Critical information assets are identified and prioritized for fast and efficient remediation where warranted. Foundstone enables total control and management over this process. SRM teams can access reports that quantify progress and dynamically rate their organizations' security posture to all levels of management (IT, security and line-of-business professionals).

Foundstone's risk assessment and management solutions activate continuous protection of the right assets, from the right threats, with the right measures. The optimal balance of software, people and processes are put in place to support rapid change while maintaining business and IT stability. Solutions are supported through open standards, best practices and continuous improvement.

The specific elements of Foundstone's ERS consist of:

- **Foundstone Enterprise Manager** – A Web portal that provides a centralized view of the entire vulnerability management process—from asset discovery and prioritization, to monitoring, remediation and reporting.
- **FoundScan Engine™** – This is the core scanning technology of the Foundstone distributed system. It enables asset discovery and vulnerability analysis across the enterprise.
- **Foundstone Database** – A scalable, frequently updated repository of Foundstone's knowledge base and customer data, it intelligently stores asset inventory, vulnerabilities and threats for efficient retrieval and analysis.
- **Executive Dashboard Module™** – Presents an interactive “big picture” of organizations' security health by combining all of the organization's asset value and vulnerability information into a series of graphical charts.
- **Remediation Module** – This is an integrated system for helping customers eliminate vulnerabilities, streamlining the fix process and measuring progress.
- **Threat Correlation Module** – Foundstone's forthcoming Threat Correlation Module places up-to-the-minute threat intelligence in the hands of organizations

so that they can respond immediately to breaking events. This module profiles current threats such as worms and wide-scale attacks and correlates these events to customers' asset and vulnerability information already gathered by Foundstone Enterprise system. The severity of the associated threats and vulnerabilities combined with each asset's associated value determine the risk score for each asset. Through Foundstone's asset-based risk ranking system, customers can quickly respond where it matters most, allowing threat impact to be managed or even eliminated.

- **Web server and Web application inventory** – This module crawls web servers and their contents in order to identify and analyze their contents, resulting in a categorized listing of Web servers and the objects residing on them.
- **Source-Sifting** – Provides detailed analysis of the source of scripts and static pages discovered on analyzed Web servers that reflects discovered database connection strings, e-mail addresses, hidden form fields, and other potentially sensitive items.
- **Authentication Testing** – Discovers weak usernames and passwords (easily guessed or default accounts) over HTTP Basic, NTLM, or unacceptable forms-based authentication.
- **Source-Code Disclosure** – Through a combination of missing Web server patches or misconfigurations coupled with the Web application inventory, Web scripting source code can be presented to an attacker, revealing potentially sensitive information such as database connectivity details or even usernames and passwords.
- **SQL Query Misuse** – The SQL usage testing component of the Web application module tests for improper handling of erroneous queries that result from failure to conduct input validation within the application. Failure to remediate this can result in attackers gaining information that can be used to mount more aggressive attacks.
- **Smart Guesswork** – Encompassing many types of security probes, Smart Guesswork searches for files and directories that are obscured to the normal user but available on the Web server when exhaustive testing is undertaken. Examples of probes used include searches for default directories, hidden archives, and often sensitive files such as robots.txt that either possess privileged data or point to where it can be located by an attacker.

For more information on how to implement SRM strategies, or to learn how Foundstone's ERS offerings can enhance an organizations risk posture, contact Foundstone at:

27201 Puerta Real, Suite 400
Mission Viejo, CA 92691
877.91.FOUND
949.297.5600
ERS@foundstone.com
www.foundstone.com