



AberdeenGroup

Turning IT Security into
Effective Business Risk
Management

An Executive White Paper

July 2003

Aberdeen Group, Inc.
260 Franklin Street
Boston, Massachusetts 02110-3112 USA
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

Turning IT Security into Effective Business Risk Management

Executive Summary

Security data, which is here, there, and everywhere, is not yet tangible and accurate enough to pinpoint the risks of using technology to automate business processes. Whether extending regional hubs, integrating the information technology (IT) operations of a company being acquired, using a new network carrier, or opening new off-shore offices, business decision makers need to know the risks of using technology to make enterprises' business processes more effective.

An all-too-common "we'll find out" stance, although honest, is unfortunately not the most often quoted response. Instead of looking unprepared, IT organizations prepare "guesstimates" in the hope that bullets can be dodged in the future. The "we really don't know" condition plaguing most firms is rooted in several conditions, including:

- Short-staffed IT organizations and a lack of tools
- An inability to easily discover and integrate mountains of data from a wide variety of currently deployed information systems
- A lack of business-focused risk management applications that can turn data into meaningful and actionable information

Security information management (SIM) is positioned to address these gaps while delivering the insights needed for assessing business risk and technology vulnerability. Currently focused on collecting and organizing data about security-related events, SIM products can be thought of as an electronic card catalog system for security events. If this were all that it accomplished, SIM would be a major improvement in efficiency and awareness, especially compared with the current state of intrusion detection systems (IDS) that overwhelm IT staffs with too much data and little actual knowledge.

Unfortunately, some SIM products are impaired when it comes to finding problems that are directly related to critical business and application systems. Blind to business asset value and non-security-event data, some SIM products obfuscate risks that are involved with "business" systems that the enterprise relies on for operating its core missions.

Capabilities being added by suppliers will take SIM-based security monitoring to the next level: the management of business risk associated with the day-to-day use of technology.

However, capabilities being added by suppliers of these security management systems will soon take SIM to the next level: the management of business risks associated with the day-to-day use of technology deployed in IT production operations. During 2003, SIM products will mature into tools for managing the business risks associated with the use of technology systems. Some capabilities being added to

SIM include the business relevance of IT systems; business value of IT systems; service level and business continuity views based on integrity, availability, and risk values; workflow alerting based on job function; and business risk by aggregated views of systems and business processes.

In short, the new face of SIM will enable multiple disciplines in the enterprise to manage business risk across the enterprise, including the unique forms of risk management practiced by legal, financial, auditing, IT operations, IT planning, human resources (HR), and corporate compliance functions. Not limited to security events, 2003 will also usher in expanded coverage as SIM products include most popular application systems, databases, and common application gateways, such as e-mail and Web servers, among others.

This *Executive White Paper* looks at the current state of SIM, analyzes some of the drivers behind early SIM deployments, provides insight into some new capabilities being added to SIM, and provides an analysis of why SIM is positioned to deliver much larger value to the enterprise as a platform for consistent IT-based business risk management practices.

SIM Drivers: Scarce Resources, No Tools, and Security Information Overload

The current interest in SIM is being driven by the combination of inadequate human resources in IT, a lack of tools for automating security event collection and analysis, and security information overload.

Security information overload is the biggest problem facing IT organizations.

Of these, security information overload is the biggest problem facing IT organizations. And the offender contributing the most to security information overload is the voluminous data being collected by security gateways, including IDS, IDS sensors, network routers, and firewalls.

Unfortunately, most security event data collected by these network devices is noise. Interviews conducted by Aberdeen during the past year indicate that the number of security events collected by network gateways is easily exceeding tens of thousands per month. Nearly 90% of this data is considered undifferentiated background “noise” and chatter that has little security and no business risk-related relevance (Figure 1).

The biggest problems cited by IT executives and security specialists alike include:

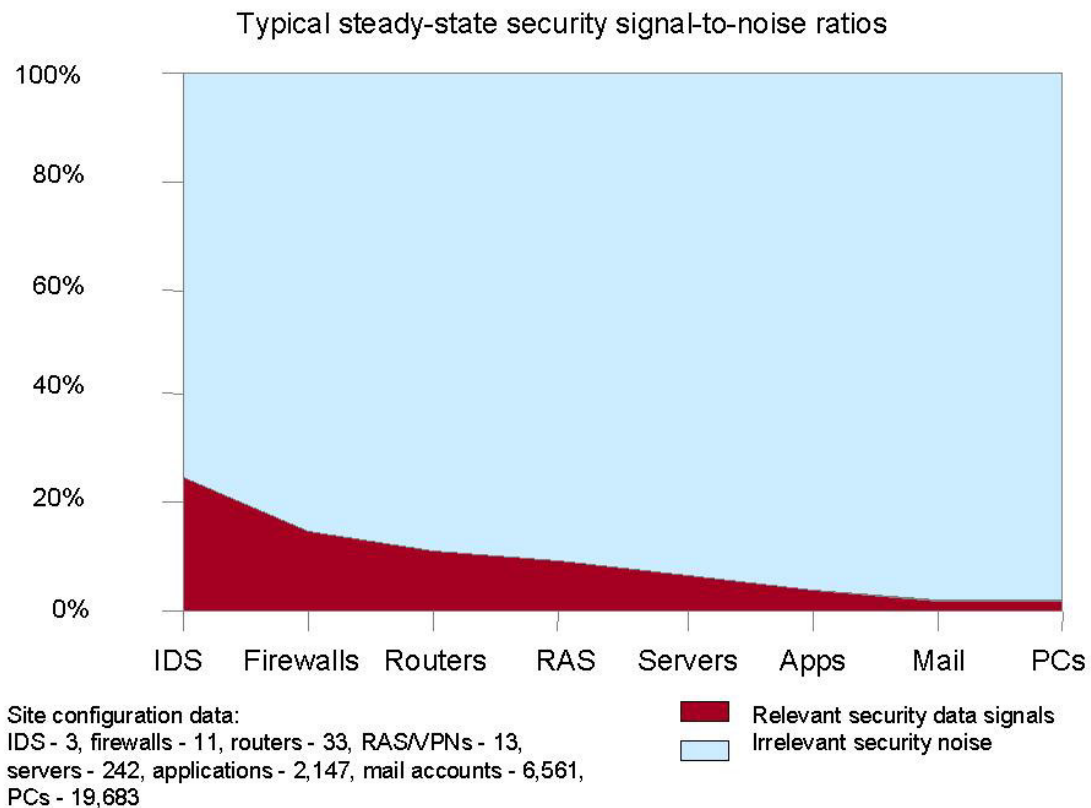
- Security audit information overload is acute for “network” devices.
- Audit data contained in local business systems is often inaccessible or difficult to obtain.
- Separating business risks from background “noise” is nearly impossible.

The reality is that security information overload is far beyond the capacity of any organization to deal with successfully. Even if firms could hire enough people to baby-sit every security event, it would be fruitless: Not only is hiring more people a bad use of capital, but electrons, bits, and bytes always flow much faster than people can operate. The intersection of scarce human resources, information overload, and no tools is being solved by SIM applications that consume mountains of security and audit data, make sense of the data, and then make it possible for a small staff to leverage its technology automation capabilities.

Event Data and the Technology Chassis Driving SIM Applications

SIM applications can be driven by any “event.” For too long, suppliers of security gateways attempted to convince IT buyers that a distinction existed between “network events” and “host events.” This marketing distinction reached its zenith when suppliers of IDS sensors were trying to capture market share in the late 1990s. The marketing cacophony from this effort remains with us to this day.

Figure 1: Security Information Overload



Source: Aberdeen Group, July 2003

The technology reality is that network devices, such as IDS sensors, routers, and firewalls, are also hosts, albeit special-purpose-built hosts. And their special purpose is focused on network services, ports, and protocols. No matter what the source, the core building block of auditing and event monitoring feeding SIM applications is based on perimeter event triggers, which includes a wide range of technologies. Some of these technologies include signature patterns, database audit masks, application logs, SNMP traps, and RMON (remote monitoring) events.

From the perspective of SIM, every IT application and device, as well as vulnerability and threat databases, are a source of rich event data from which to pinpoint value-based risk. In this respect, SIM is invariant to whether data is coming from “network” events, “database” events, “application” events, special-purpose hosts that are attached to the network, or databases of known vulnerabilities and threats. SIM applications apply intelligent analysis to the type, source, and contents of event data regardless of source. Although SIM applications take into account the special purpose of IT devices and data sets, SIM analysis is agnostic with respect to sources and methods of collecting data. And it needs to be because the volume of data and noise continues to expand with time.

Early Phase SIM Systems — Prior to 2003

SIM systems were first available in 1999. Over a four-year period, many of these systems developed a comprehensive set of agents that could be deposited on local devices for the purpose of collecting security event data, as well as interfacing with most popular network security gateways, including IDS sensors, firewalls, network routers, and some VPN routers.

In large part, these systems focused — almost exclusively — on the collection, aggregation, and correlation of security event data. Delivering correlated data across the enterprise network, the presentation services of early SIM products were limited to numerical, tabular, and graphical renditions of security events (Figure 2).

Moving beyond a flat presentation of network-based security event data, these products evolved to include more meaningful graphics and alerting services. A few incorporated color-coded graphics to assist IT managers with priorities for response and mediation efforts. Many of the early SIM products included applications that analyzed network security event data based on conceptual forms of risk. However, the early SIM products displayed several drawbacks, including:

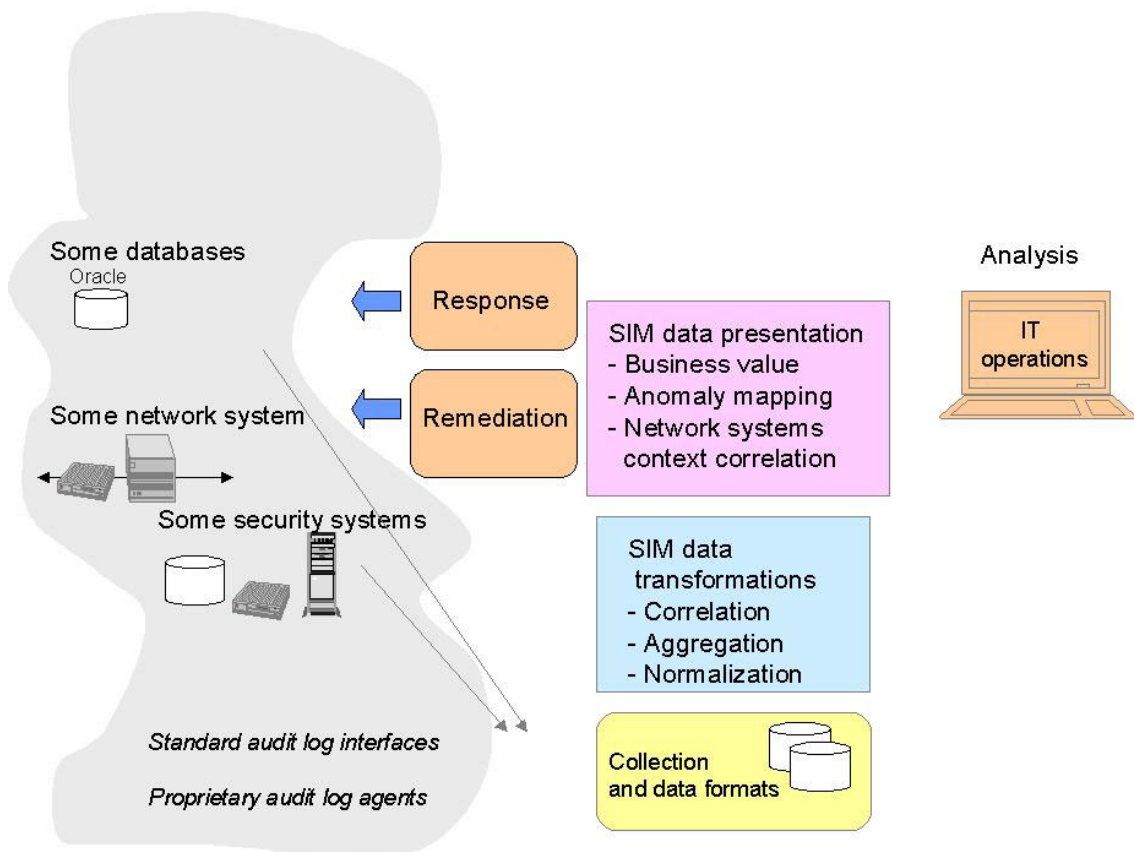
- There was no business-based value adjustment of security event data.
- Highly skilled network security engineers were required to interpret the results.
- Views of risk — beyond IT-based network events — were not considered.

Although this characterization of pre-2003 SIM systems is not universal, it is a fairly good way for most of them to be considered. However during 2002, many of the leading SIM suppliers started listening to customers and started acting on their requirements. The results are now showing up in products that are — and will be — available in 2003.

SIM-Based Security Management Systems: 2003 — and Going Forward

SIM applications are voracious consumers of whatever event data set is plugged into them, including live event data from any source connected to the enterprise network and from any known vulnerability and threat data set. In 2003, leading SIM systems include the asset values of IT resources under management, the business value of these resources and their related business processes, the business risk if these assets are threatened, and the risk to the organization if these IT resources are not available or are compromised.

Figure 2: Early Phase SIM Systems, Prior to 2003



Source: Aberdeen Group, July 2003

By focusing on the intersection of business asset values, threats, and vulnerabilities, SIM solutions in 2003 will help the enterprise to move beyond managing technology controls and into an active profile for managing business risk.

By focusing on the intersection of business asset values, threats, and vulnerabilities, SIM-based security management will move the enterprise into an active risk management profile.

In addition to business value, threat, and risk being added to SIM's analytical mix, the visual and alerting output capabilities of some SIM solutions are being delivered in plug-compatible layers that make it possible to direct relevant, actionable information to a wide variety of different people across the enterprise. Thus, the unique views of risk that are analyzed by different business functions — HR, legal, auditing, IT, finance, compliance — will be made tangible (Figure 3).

SIM Data Collection and Formats

SIM applications thrive on data: the more of it the better. Finding relationships between events is much easier — and more rapid — when there is more data. The early users of SIM say that its applications thrive on information overload and remove this burden from people. Although some SIM solutions can collect data only from security devices, others are consuming security and audit-based event data from almost any recording scheme, including local audit files, hosts, mainframes, Unix and Linux systems, Windows systems, applications, databases, Web and mail servers, network devices, IDS sensors, firewalls, and network routers. Sources for SIM can also include SNMP feeds, RMON traps, and specific application programming interfaces (APIs) that are being used for extracting any audit-related data.

By correlating event data across networks, systems, applications, and transaction systems, SIM can more rapidly identify and alert relevant staff about risk conditions that have a direct impact on the business operations of the enterprise. By moving beyond “network security event data,” SIM will elevate its analytical applications beyond a technology focus into meaningful business impact.

SIM-Based Analytical Engines

Data transformations and analytics are the heart of most SIM applications that are available today. The primary tools employed for transforming “event” data into meaningful information includes data normalization, aggregation, and correlation applications.

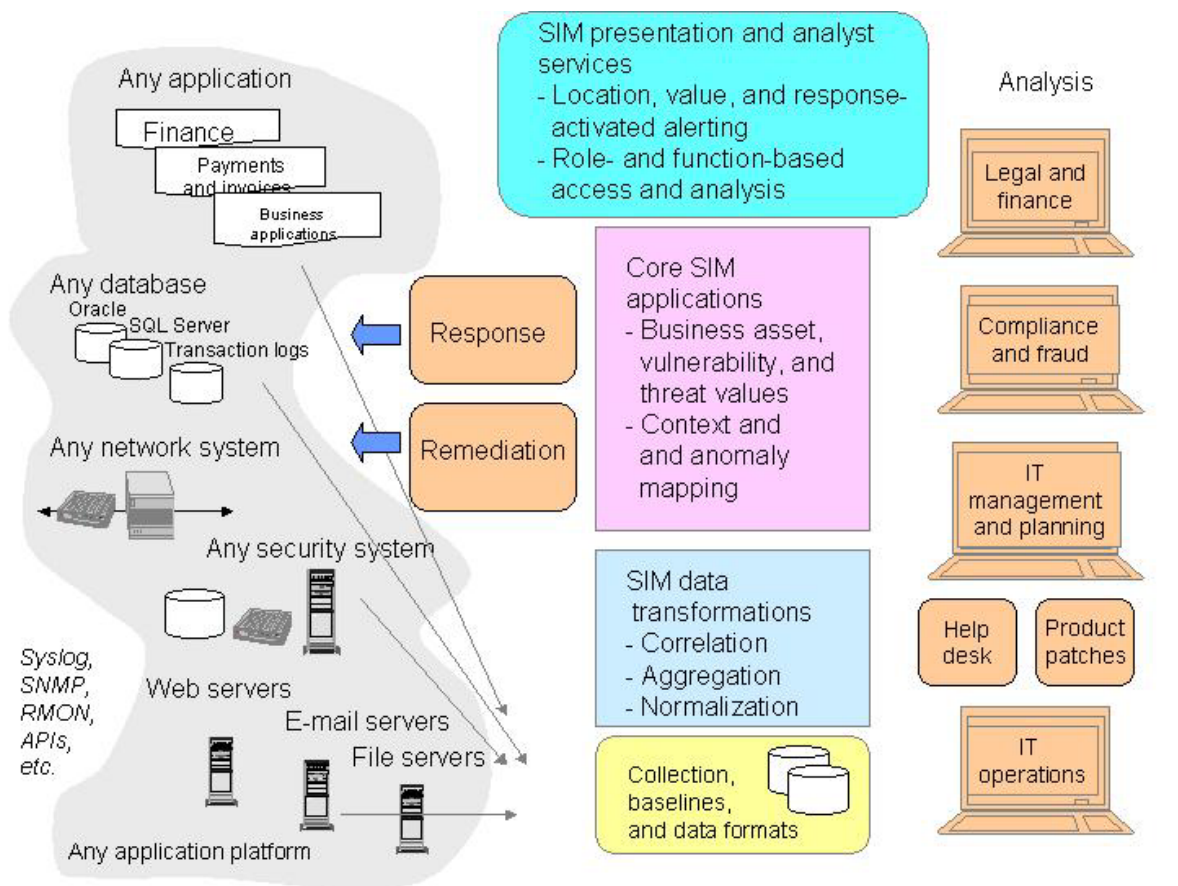
Most suppliers of SIM products currently normalize event data to ensure that its analysis applications — aggregation and correlation — can address the data in a similar manner. Most event data coming into SIM systems is formatted differently by their sources. These various formats are a little bit like the differences in data

formats from one version of Microsoft Word to another, except the data being normalized is “event” data, not word processing text. Another way to think of data normalization is that it transforms multiple “event” data languages into an Esperanto for SIM applications.

Almost all SIM solutions aggregate event data. Data aggregation takes normalized data and organizes it by category. For example, categories could be source (IT systems, applications, etc.) as well as asset value or business function. SIM aggregation takes similar kinds of event data and duplicates it into multiple categories for higher level applications to operate against.

Three primary forms of correlation are delivered by most SIM applications: rules, anomaly, and statistical correlation. Rule-based correlation delivers prepackaged transformations of event data into different “views” of the data. For example, rules can sift data by all events related to a specific trading operation, a class of transactions, and a geographic location. Anomaly-based correlation often depends on a

Figure 3: Business-Focused SIM Systems, 2003 and Beyond



Source: Aberdeen Group, July 2003

set of “baseline” data that is collected by the SIM system from a “learning mode” during which a database of measured events is built. Often operated for a number of weeks, “baseline” snapshots are then compared with current events to determine whether anomalies from baselines are occurring. In the future, baseline capture must be operated in a heuristic steady-state mode if it is to deliver value for a constantly changing IT and business transaction environment.

Current statistical correlation techniques are providing useful insight, especially for time-based events. Beyond time-based events, however, statistical correlation is currently a learning process for many buyers and suppliers. Fortunately, new applications are being added to SIM based on requirements from internal auditing teams that commonly employ hypothesis testing and statistical analysis.

SIM Presentation and Analyst Applications

Almost all SIM products deliver powerful presentation and visualization capabilities to empower people to “see” the proverbial needles in the haystacks. Typically, SIM products provide different views of the data, including visual views of the entire enterprise network, drill-down views into specific application servers, cross

The more compelling view that SIM will deliver is the impact to the business versus the likelihood of attack.

views of rule-based correlated data, and statistical views that show changes from optimum risk levels. Some of the newer features to look for include color-coded alerts, risk forecasting, policy deviations, geographic maps, topographic projections, architectural mappings, application loading, unusual “blips” in transactions, building egresses, and electronic systems access points. SIM will also be delivering the “impact to the business” against “likelihood of attack,” a simple but effective view of business-based risk that will enable the enterprise to

more easily prioritize corrective action based on its unique needs.

Focused Business Value and SIM

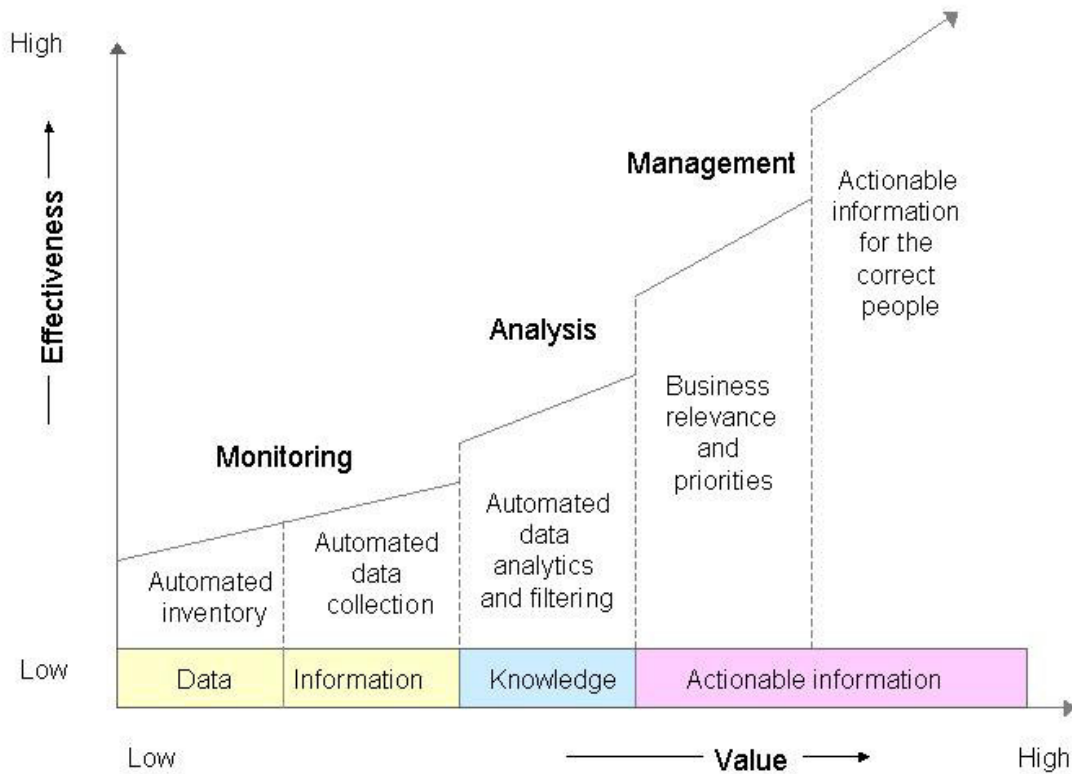
The newer views of business risk being delivered with SIM-based risk management tools are due to their ability to map the business value of IT systems to the organization. Often simplified by business function, this ranking makes it possible to associate value with clusters of IT resources, applications, and data. For example, after auto-discovery, some SIM applications provide users with the opportunity to color-code collections of IT systems — around the world — that are being used for customer service, manufacturing, distribution, order processing, invoicing, credit operations, sales, accounting, human resources, and other business functions. These “business functions” are then assigned “value” in the organization based on the functional responsibilities performed by different people based on their job function.

Collating IT systems used by business function and assigning business value to these systems enable firms to focus their response and remediation efforts to prioritized business needs. Instead of treating every event as equal, SIM delivers a “business risk” bias to event data, based on the business uses of technology and thus delivers greater value to the organization (Figure 4). When cross-tabulated by business risk and priority — should these systems become unavailable or compromised — SIM applications can distinguish between prioritized business-related risk versus nonemergency signals and events that can be addressed at a later time.

Access to Views of SIM Data Based on Appropriate Job Function

Applications new to SIM are delivering views of event data through virtual portals with preconfigured application and data rights, based on job function. Although it might be appropriate for security administrators in IT organizations to be dealing with security events from firewalls, IDS sensors, and network routers, they are

Figure 4: Value of SIM: Actionable Information for the Correct People



Source: Aberdeen Group, July 2003

probably the wrong people to be accessing data that relate to financial records, customer records, and other sensitive business transaction data.

Similarly, compliance managers can be provided with data that is relevant to their jobs, while auditors can be provided with detailed data appropriate to their function. Likewise, financial and legal officers can be provided with important summary views of business-related technology risks without being overloaded with data. SIM delivers the ability to provide everything from summary views of risk to the agonizingly detailed data that might be needed by compliance managers, auditors, and IT managers who are in charge of applications, networks, operations, security, and data storage systems.

Worms to Look for Underneath Some SIM Rocks

To date, there are about 20 different SIM and SIM-like products on the market, a rather rapid development in a short four-year time frame. The development SIM technology has resulted in some big differences in the products being offered by suppliers. Here are some of the salient differences — and hidden items — that buyers need to consider as a part of their evaluation criteria.

Collecting Actual Event Data

Some SIM applications record only security-relevant events coming from IDS sensors. Others include audit data coming from related network security gateways. Still others include data from almost any application system on the network. The differences result from the technologies that the supplier may be using to interface with and collect audit events. Suppliers whose SIM products collect only network security event data are probably using standard output logs from these devices. Often requiring IT managers to deploy interceptor agents, these solutions will help IT organizations to overcome the overload of data from IDS, firewall, network router, and similar gateways. However, network security SIM systems are only capable of correlating data across these security systems in the enterprise. Unfortunately, they are blind to mission-critical business systems, databases, and applications that run the business. The analysis engines of these SIM solutions can only guess at business value because there is no relevant data upon which their analytic engines can operate. However, suppliers whose SIM products are collecting data from any device are more likely candidates that are — or will soon be — delivering the capabilities that turn SIM into tools for managing the business risks associated with the use of technology.

Lack of “Open” Sources of Data

A difficulty facing all SIM suppliers is the lack of an “open” Esperanto standard for audit and event trail data. The lack of a standard format for threat, vulnerability, audit, and event data — across the many stovepiped technology systems employed

by the enterprise — is the reason all SIM suppliers are forced to spend engineering resources to normalize data before running any analytical applications on collected data.

Signature Patterns and Actual Event Data

SIM suppliers proposing to deliver a solution based entirely on signature patterns are not going to be able to deliver anything beyond a software engineer's view of risk. For SIM to work its magic, it must collect live event data. Signature patterns are useful when sufficient information on correlated events indicates conclusively that pattern matching will always result in faster positive identification. As a result, signature patterns should be considered as an augment to live event data, not as a complete substitute for actual conditions.

Moving Beyond the Card Catalog

Some SIM solutions are currently unable to automate business risk analysis because their analytical engines do not yet account for the business value of the IT systems being monitored. Although these “card catalog” solutions are solving many problems in IT organizations, their underlying aggregation and correlation functions are not appropriately biasing “event data based on “value.” Moving beyond the card catalog, these solutions will need to add several capabilities, including:

- Multiple views of event data, based on job function
- Value-based analysis applications
- Data sources that are more inclusive than just security events

Moving Beyond Security Event Data

A few of the leading SIM products are now collecting event data from popular application systems (e-mail, Web, HR, finance, transaction systems, customer relationship systems, etc.). Many SIM solutions will add the necessary event collection capabilities and business value analysis focus to their product mix during 2003, making it possible for IT staff to compare a number of options.

Additional Advances in SIM: Coming to Your Neighborhood Soon

Suppliers are adding new capabilities — this year — that promise to make the value of SIM even more compelling beyond being able to industrialize security and risk management processes in the enterprise.

Some of the new features of SIM to look for, include:

- A comprehensive “learning mode” that continually rebuilds what constitutes “normal”

- Active and simulation “modes” that make it possible to operate SIM in production environments while testing changes prior to deployment
- Open sources for asset value, event, risk, vulnerability, and threat data sets
- Integration with any system being used for repair and remediation

New standards for “open” audit event trail data will make it easier for IT buyers to find a larger choice of advanced business-focused SIM solutions. Industry-standard, “open” event collection methods will allow suppliers to rededicate engineering resources to analytics and presentation services, rather than to the many specialty agents for collecting data that would be required otherwise.

In addition, suppliers will be adding new, graphically rich views into SIM-based risk analysis based on a user’s job function. With the introduction of these capabilities, buyers will be able to graphically “point and click” entire topographic sections of the enterprise’s IT infrastructure into “value” and “risk” zones that have meaning for how the enterprise conducts its operations and how it values those operations.

Rather than being confined to predetermined value concepts, the new features of SIM will make it possible for each enterprise to quickly make SIM a part of its business risk management fabric for its organization. Moreover, the multiple business-focused “views” of risk promise to assist the most common risk management functions in the enterprise to do their jobs better, faster, and with much more accurate information.

The new capabilities being added to SIM systems, especially their visual renderings of the impact to the business versus likelihood of threat means that it will be possible for the enterprise to measure and effectively reduce risk occurring in its business operations. Not constrained to a simplistic technology view of risk, the enterprise will be able to immediately see its business value. As a result, the new capabilities of SIM will enable firms to make effective progress in reducing business risk from the use of technology to acceptable levels (Figure 5).

Aberdeen Conclusions

According to SIM users, the new capabilities being delivered with SIM solutions during 2003 are delivering expanded value, including:

- The “state of risk” is being measured and made visible.
- Actions to reduce risk are based on empirical evidence.
- Threats and vulnerabilities are being prioritized.
- Risk events are being brought closer to “real time.”

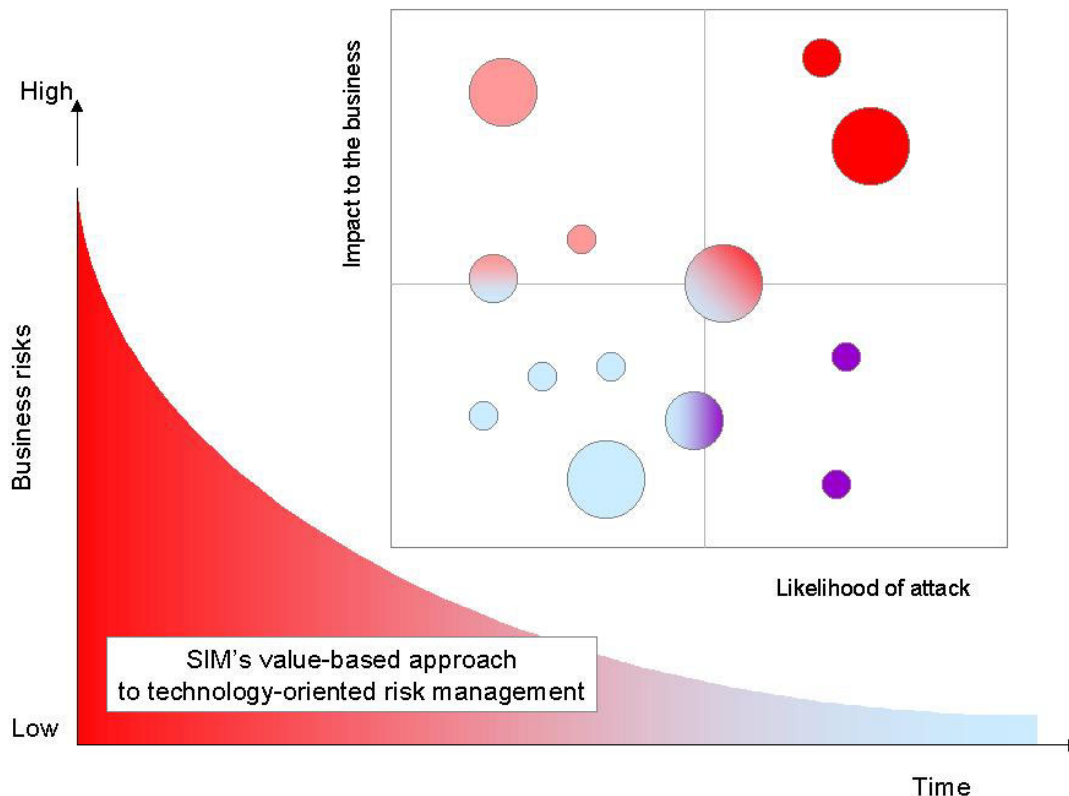
Although focused in the past — rather narrowly — on security events, SIM systems in 2003 will make it possible for the IT executive, financial officer, legal counsel,

internal auditing teams, the board of directors, executives, and senior business managers to more easily see and manage tangible risk. Moreover, new applications being added to SIM during 2003 will also enable IT managers to increase service levels for systems and networks under management.

With the new business views delivered by SIM in 2003, only the most important events need to be attended to and repaired immediately. The “business-focused” view of IT risk will enable auditing, legal, HR, business, and IT staff to become more productive, and with fewer resources.

The current users of SIM systems say that they foresee the day — just ahead — when these security and risk management solutions will enable their organizations to focus on real problems and the risks associated with technology systems that are used to operate the business. Planning to shift their spending from technology plumbing to risk management, these firms will be well positioned to stretch the

Figure 5: Turning IT Security into Business Risk Management



Source: Aberdeen Group, July 2003

envelope of SIM-based risk management to operate the business, by being able to react to, as well as predict, the business impacts and risks associated with the uses of technology.

The advances to SIM-based risk management during 2003 are a watershed event for IT buyers and suppliers alike. For buyers, the business-focused value analysis being delivered through SIM promises to lift the security function within IT out of the dark arts and place it on an empirically based scientific footing that can be used to help drive the business. Moreover, SIM promises to deliver data that will enable buyers to more adequately determine where to spend additional money on managing risk, based on business need, not conjecture. Buyers should be looking for a supplier with domain expertise in business value asset applications, information management, and “open” security systems.

For suppliers, SIM promises to realign the industry landscape along very different lines than is currently the case. Although this will be wrenching for some, those who are prescient enough to understand the impact that SIM will play will have the opportunity to service a more knowledgeable — and pragmatic — set of customer requirements in the future.

Those who are already familiar with the business value mix inherent in the new applications of SIM-based security management are planning to leverage it as much as possible.

Those unfamiliar with SIM will be well served to find out what their peers know and why they plan to take advantage of it — this year.

To provide us with your feedback on this research, please go to www.aberdeen.com/feedback.

*Aberdeen Group, Inc.
260 Franklin Street
Boston, Massachusetts
02110-3112
USA*

*Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com*

*© 2003 Aberdeen Group, Inc.
All rights reserved
July 2003*

Aberdeen Group is a computer and communications research and consulting organization closely monitoring enterprise-user needs, technological changes, and market developments.

Based on a comprehensive analytical framework, Aberdeen provides fresh insights into the future of computing and networking and the implications for users and the industry.

Aberdeen Group performs projects for a select group of domestic and international clients requiring strategic and tactical advice and hard answers on how to manage computer and communications technology. This document is the result of independent research performed by Aberdeen Group. It was underwritten by Computer Associates International, Inc. Aberdeen Group believes its findings are objective and represent the best analysis available at the time of publication.