Assets, Threats and Vulnerabilities: Discovery and Analysis

A comprehensive approach to Enterprise Risk Management

By

Symantec Corporation

Executive Summary

Over the past decade, the state-of-the-art in network security has evolved from its initial focus on point solutions, such as firewalls and encryption, through a second-generation of technologies that aimed primarily at identifying the entire universe of potential vulnerabilities within a network. As information networks and the organizations that they support have become more far-reaching, heterogeneous and complex, the limited scope of point products and the brute force of vulnerability probing have now both fallen short of meeting the needs of most large enterprise environments.

As the third wave in Network Security is emerging, it has become clear that truly effective security measures must take a more comprehensive perspective, by providing a foundation of security information and support tools that allow the organization to interactively assess, prioritize and manage all aspects of protecting its vital information. Such comprehensive assessments must go well beyond just cataloging all the potential vulnerabilities, as has been the focus of second-generation scanning and probing tools. Such third-generation solutions must provide robust enterprise-wide comprehensive business driven risk assessment capabilities.

These next generation Network Security Management Systems have to empower decision-makers at all levels, such as security managers, network administrators, CIOs, CFOs, etc., with quantifiable data regarding all three key aspects of the Risk Equation – including:

- Development of a value-graded inventory of all information system **Assets**
- Definition of multi-faceted profiles of potential **Threats** to critical real-world business functions
- Comprehensive enterprise-level assessment and mapping of actual **Vulnerabilities** to the corresponding Threat and Asset rankings

In addition to needing a structured, comprehensive, asset-driven, risk-assessment methodology, the various levels of corporate staff also require flexible easy-to-use analysis tools that can allow them to model and refine the tradeoffs associated with various security measures. For instance, from a CIO's perspective, it isn't very useful to have an exhaustive listing of every potential vulnerability without the decision-support tools to help define and rank the actual threats and potential costs associated with each one. Or from a network administrator's perspective, a vulnerability or threat listing that cannot be easily mapped to the actual topology of their current network assets is likely to raise their fear level but doesn't do much to help define a plan of action.

The balance of this white paper will provide more detail on the evolving requirements for comprehensive asset-driven network security management, the enabling technologies, and the immediate benefits that can be achieved through these third-generation decision-support systems. In addition, we will provide background information outlining the specific expertise, capabilities and mission of Symantec Corporation plus a brief product overview of the Expert 4.1 risk assessment and analysis system.

Evolution of the Network Security Market

Soon after organizations first began to rely upon networked computer environments to enhance the creation, storage, communication and use of vital information, critical concerns arose regarding the protection of that information – from either unauthorized access and/or potential destruction. As with many product evolutions, the network security industry focused initially on shoring up the most glaring security weaknesses, then progressed from there to identifying other vulnerable areas needing attention.

Point Solutions – Such as Firewalls and Encryption

The first generation of network security measures focused directly upon addressing the obvious vulnerabilities. Firewalls were originally designed because the ever-expanding connectivity of computer networks posed the clear risk of unauthorized intrusion. The basic premise of firewall technology is to segment the network into "protected areas" by establishing guarded gateways that are intended to keep the users and information on the inside safe from access by non-authorized users from the outside. Encryption on the other hand was simply intended to prevent unauthorized users from being able to read vital information even if they did get access to it.

The major shortcoming with point solutions, such as firewalls and encryption, essentially lies not in what they can or cannot accomplish, but rather in deciding when and how best to employ them. For instance, a single network with one gateway to the outside world might lend itself to a fairly straightforward intuitive assessment of whether or not to deploy a firewall. But for most of today's larger organizations, the information networks consist of a myriad of internal networks and backbones populated by a heterogeneous mix of client desktops, applications servers, database/storage servers, remote dial-up servers, public-network access points, desktop dial-up modems, Intranet services, Internet presence, etc. Long ago we left behind the time when a security manager or network administrator could reliably deploy their point solutions on merely a "gut-feel" basis.

Intrusion-Driven Scanning for Vulnerabilities

The sheer variability and complexity of such network environments led to the development of more sophisticated mechanisms for identifying the vulnerable areas that required attention. A new category of products quickly emerged that essentially consisted of "scanning" and "probing" systems. These products were aimed primarily at finding the network's weak points through application of a variety of intrusion scenarios.

Scanning & Probing Products

The concept of scanning and probing initially appeared as hacker-oriented "free-ware" products, such as SATAN, COPS, Trip Wire, Strobe, etc., from which evolved a number of commercially supported products. The basic focus of scanning is to simply identify as many of the systems' vulnerabilities as possible by actively attempting intrusions at many different points. While most of today's commercial scanning products do a very credible job of identifying vulnerabilities and the counter-measures or safeguards that can be used

to address them, their ranking mechanisms don't go much beyond relatively course gradations, such as High, Medium and Low priority. From a decision-support perspective, these second-generation systems also rarely include any capability for modeling different safeguard scenarios and/or conducting cost-benefit analysis of the proposed counter-measures.

Potential Negative Impacts of Invasive Probing

Another concern that has arisen with regard to scanning tools is the potential harmful effects that can result from the use of invasive "brute force" probing methodologies. As with the first tenet of the medical profession, network security products should have a primary goal to "do no harm" to the systems and organizations that they are serving. In a significant number of cases the mere application of simulated attacks through the use of intrusive probing can actually cause unintended system failures. Given the high cost of downtime and productivity loss associated with most mission-critical systems, system managers simply cannot afford the untargeted usage of an analysis tool that might find a potential vulnerability by inadvertently turning it into a catastrophic failure.

Intrusion Detection Systems

Another aspect of second-generation network security methods is the evolution of Intrusion Detection Systems, which proactively identify and track patterns of activities that can signal potential intrusion attempts and/or misuse of the information environment. Much of the pioneering work on intrusion detection systems was carried out by the current technology staff of Symantec Corporation as part of contract efforts between Trident Data Systems and the US Air Force Information Warfare Center (AFIWC) at Kelly Air Force Base in Texas. A significant result of this early work by today's Symantec technical staff was the implementation of the Distributed Intrusion Detection System, currently in use throughout Air Force installations worldwide.

Much of the groundwork that went into our pioneering intrusion detection efforts consisted of the development of comprehensive methods for defining potential Threats as well as algorithm-driven techniques for quantifiably relating both Threats and Vulnerabilities to the actual criticality of specific Assets throughout the network. The further refinement and extension of these concepts for managing Total Risk Assessment have now formed the foundation for the next industry transition toward comprehensive Generation 3 Network Security Management solutions.

Generation 3 – Network Security Management

The basic thrust of third-generation network security solutions is to bring together all of the pre-existing capabilities into a comprehensive management-oriented capability that allows rational security decisions to be effectively interwoven with the organization's overall mission, goals, and business objectives. The ultimate goal is to be able to make network security risk-management an integral component of the organization's basic tool set for on-going day-to-day management in line with its strategic goals. Rather than

constituting a limited scope activity or a point-in-time event, truly effective security management must be able to provide a top-down comprehensive context for more appropriately deploying specific scans, tests, analysis methods, safeguards and other counter-measures.

Driving Forces – Global Standards & Regulations

Over the past few years the emphasis among leading regulatory and standards-setting organizations within the security environment has been toward the definition and establishment of comprehensive risk management systems. For instance, the British Standard BS7799 defines over 100 specific structured security guidelines in its Part 1 Code of Practices, but now also has added a Part 2 Management Standard that also specifies a management framework, objectives and control requirements for information security management systems. Similarly the U.S. Critical Infrastructure Assurance Office (CIAO) was established by the President in May 1998 to "facilitate the creation of a national plan to protect the services that we depend on daily: telecommunications, banking and finance, electric power, transportation, gas and oil, emergency services and government services." In addition, the US General Accounting Office has produced a detailed report that outlines a compendium of "best practices" while also recommending the establishment of structured systems for managing information security.

Ultimately, this emphasis on the "management methods" employed for ensuring information security appears to be moving the industry toward a process-certification system, potentially analogous to the ISO-9000 certification system used to ensure the integrity of Quality Management methods. As a matter of fact, BS7799 has already been adopted by a number of European countries and is being proposed as an ISO standard. Regardless of whether these emerging management practices remain as recommendations or evolve into mandates, it is clear that in the near future organizations will be held accountable for the rationale of their security management as well as its results. The ability to demonstrate appropriate "duty of care" measures will become critical factors for avoiding corporate liabilities and successfully meeting business objectives.

Asset-Driven Risk Assessment

From an enterprise-wide perspective, the structured management of overall security risks must invariably start with an understanding of the relative criticality and value of all the organization's information assets. Only by first identifying, cataloging and analyzing all of its assets can the organization assess the impacts of their potential unauthorized destruction or compromise. The valued-asset inventory then provides an appropriate context for judging the real risks associated with the potential vulnerabilities and threats to those assets. True third-generation information-security management tools, such as Symantec Corporations Expert 4.1 system are able to provide rational decision-support systems by building all subsequent analysis and actions on a solid foundation of asset-driven assessment, based on enterprise-level risk assessment systems and comprehensive business-focused threat and vulnerability databases.

Symantec Corporation

Company Background

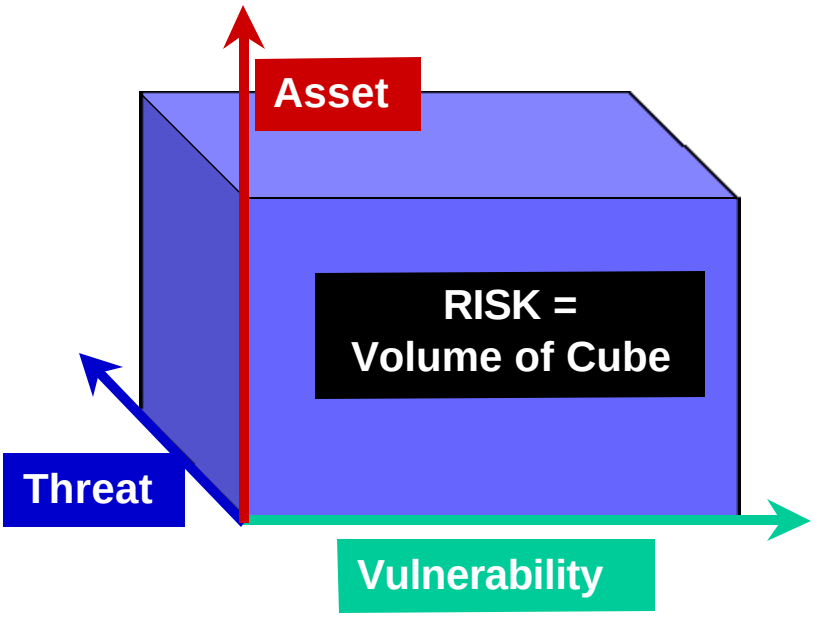
Symantec, a world leader in Internet security technology, provides a broad range of content and network security solutions to individuals and companies. The company is a leading provider of virus protection, vulnerability assessment, Internet content and e-mail filtering, and mobile code detection technologies to enterprise customers. Headquartered in Cupertino, Calif., Symantec has worldwide operations in more than 24 countries.

Expert 4.1 Product Overview

Expert 4.1 is a true third-generation network security analysis and management solution that provides comprehensive decision-support capabilities for all organizational levels and functional areas. By allowing users to quickly and easily discover all aspects of their network, identify informational assets and then define and map vulnerabilities and threats, Expert empowers both technical and non-technical users with the vital business-oriented information needed for rationally allocating security investments.

Risk = Assets x Threats x Vulnerabilities

Expert builds upon L-3 Network Security's pioneering work that established comprehensive threat definitions and detailed algorithms for conducting Total Risk Assessment. Essentially, these algorithms assist the user in quantifying the combination of asset criticality, threat level and actual vulnerability for every informational asset in the network. By representing the total risk as the volume of a cube defined by all three of these factors, Expert helps the user to quickly determine which assets require attention and also to model which counter-measures and safeguards can have the greatest impacts on reducing overall risk.



Comprehensive Database of Always-Current Security Information

To aid in accurate analysis and data-driven decision-making, Expert also contains the world's most comprehensive safeguard and vulnerability database. Symantec Security professionals are continually researching, verifying and cataloging the most recent data available in both public and private domains. New information is updated and distributed monthly to registered users of Expert so that their on-going decisions are always based upon up-to-date information.

Currently the Expert 4.1 database includes:

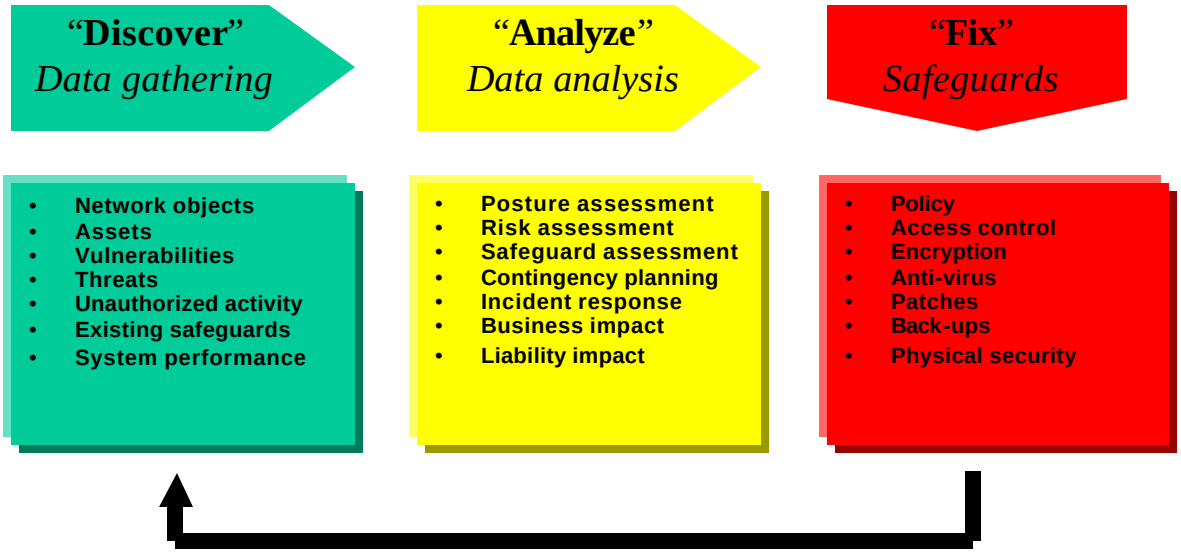
- Component information on hardware, operating systems and software from over 200 vendors
- Vulnerability information on design, administration and implementation weaknesses that can make systems vulnerable to potential attack
- Threat information that helps the user categorize potential human threats according to various levels of skill, motivation and access to the computing environment
- Safeguard information on security software, devices, policies, procedures, software fixes and work-arounds intended to reduce risk
- Business Specific data to assist users in mapping their security analysis efforts to targeted functional areas, such as manufacturing, finance, engineering, etc.

Non-Intrusive Network Mapping and Analysis

The heart of Expert's power lies in its ability to quickly and thoroughly discover and map entire networks in a non-intrusive mode. Under direct control of the user, this process automatically scans the network, using standard protocols to find and label all devices, such as computers, routers, firewalls and printers. Expert 4.1 also identifies operating systems, active services, and software in use throughout the network environment. In addition, the software's Modem Discovery function scans phone numbers for modem connections to help identify and enforce policies on controlling dial-up access. Expert 4.1 is specifically designed to perform the entire discovery process in a non-intrusive fashion that neither runs the risk of causing harmful disruptions nor places an extra load on the network.

Iterative "Discover, Analyze and Fix" Process

Expert then builds upon the comprehensive network discovery process by providing a rich set of both graphical and text-oriented analysis tools that guide the user through various in-depth assessments of both technical and business issues. Using this logical flow, decisions on safeguards, contingencies etc. can be directly related to their impacts on specific risks as well as their consistency with overall business objectives.



As safeguards and other fixes are implemented throughout the enterprise, Expert assists the user in performing an iterative assessment of the actual impacts by re-discovering the network and providing detailed reports comparing the changes in Vulnerabilities, Threats and/or Assets.

Summary

Benefits of Network Security Management

Comprehensive network security management allows users to determine business impacts based upon the organization's specific network environment, informational asset inventory, potential threat profiles, and vulnerability assessment. Expert integrates all of these factors into a flexible decision-support system that empowers the organization's professional staff to deploy appropriate cost-effective safeguards and to continuously monitor the status of their security environment on a real time basis.

Role-based Adaptability for Different Management Levels and Functions

Expert 4.1 is specifically intended to provide role-based decision-making that allows non-technical, technical and security staff to map, assess and manage the detailed aspects of the organization's network, while also providing strategic managers (e.g. CIOs and CFOs) with quantifiable answers to key questions, such as:

- *Given the current security posture of my network, what is the annual loss expectancy due to security breaches?*

- *If a specific vulnerability were exploited, what business operations would be impacted and to what degree?*
- *What are my potential legal liabilities?*
- *What security policies must I have in place to avoid loss of accreditation or litigation?*
- *What is the precise ROI of various security policies and countermeasures? How much should I spend on security?*

In addition to putting real-time vital information in easy-to-understand formats directly into the hands of corporate staff, Expert is finding broad applicability for use by security consultants, Big-5 accounting firms, etc. As a matter of fact, the flexible user-driven network-building capabilities of Expert can even enable a user or consultant to model and analyze various network architectures and topologies prior to beginning a new implementation. In these instances, Expert can actually help users avoid security problems from the outset rather than discovering them later.

The Bottom Line

The ultimate goal of third-generation information-security solutions in general and Symantec Corporations Expert 4.1 in particular is to:

"Allow organizations to make intelligent decisions about their network security posture by giving them the ability to comprehensively assess the impact on operations if network data is disclosed, corrupted, or made unavailable."