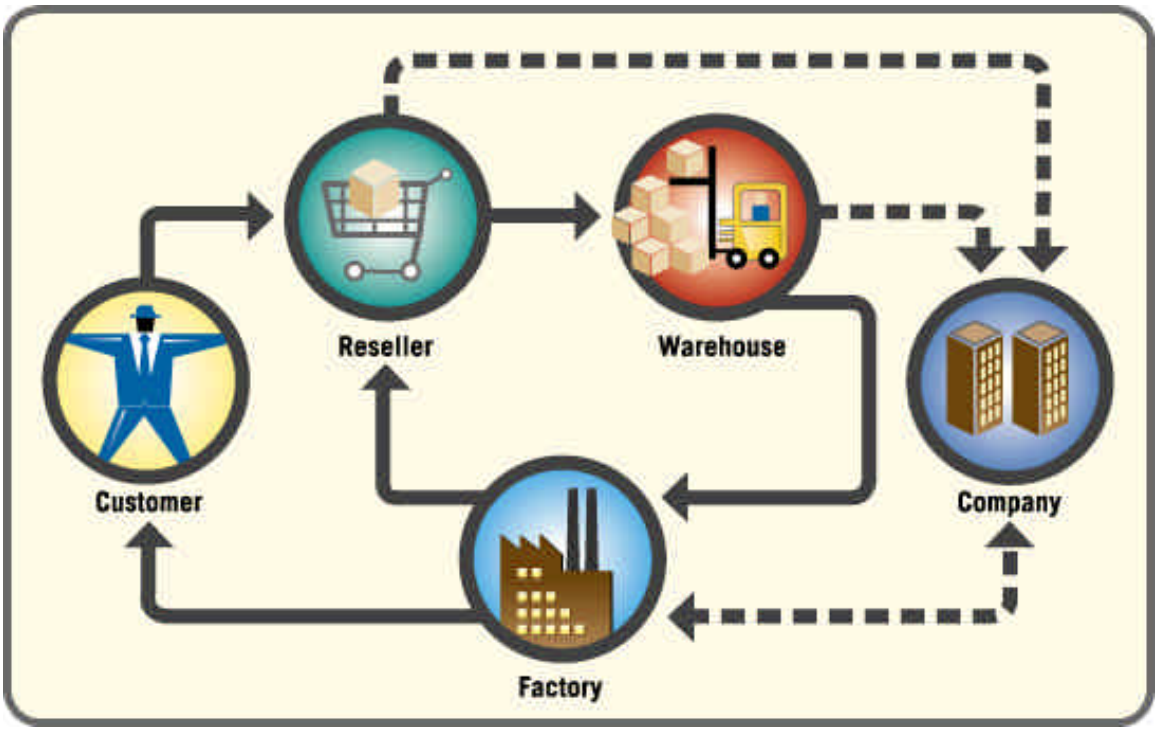
INTERNET
SECURITY
SYSTEMS

Secure E-business

New Markets at the Speed of Information;
Online Opportunities at the Speed of Thought

E-business – A Different Way To Grow

E-business is frequently misunderstood as web-based storefronts and other simple electronic services. In reality, E-business is a rich, complex mixture ranging from massive commodity exchanges to auction sites to mom-and-pop shops looking for a low-cost way to increase sales. The Internet applications software market consists of three segments: commerce sales and marketing, customer service and support, and commerce procurement/order management. This last segment is expected to become the biggest opportunity for E-business software vendors, accounting for $8.5 billion of an overall $13.1 billion market by 2003 *(Internet Commerce Software Applications Market Review and Forecast, 1998-2003, International Data Corporation/IDC*). In other words, the online stores now common on the Internet will rapidly become sophisticated Internet supply chains over the next five years.



The key to profitability in this paradigm is simple: inspire confidence from supplier to customer, be more available than possible in the physical world and protect data integrity to ensure future growth. These objectives can be met in several ways. E-business removes intermediaries from the supply chain, creating a direct, efficient link from producers to consumers. In this example, a manufacturer sells directly to customers, increasing profitability while reducing consumer costs by eliminating warehouse and reseller markups. Primary contact for service and support also moves through online channels, reducing overhead and speeding service response.

In other cases, E-business introduces an intermediary in order to create a market where none has existed before. Prominent examples of this form of online business include auction houses and online brokerages. By opening their networks to ordinary

consumers, these organizations create investing and merchandising opportunities that were previously impossible.

Finally, E-business reintegrates a market under a name brand, using that awareness to introduce branding into an otherwise fragmented business niche. Used booksellers and travel reservation services are prominent examples of this process. The value in this model comes from uniting many back-end vendors into a single branded identity. These businesses may or may not deliver the best possible price, but both suppliers and customers find the convenience of a single point of contact worth the exchange.

Aggressive organizations use their online presence to reinforce – or reinvent – their identities from the physical world. E-business, therefore, gives corporations a single set of tools that quickly adapt to new situations and opportunities. The key to profitability for all three strategies is ensuring data integrity, guaranteeing service availability and protecting confidentiality along the length of the entire online supply chain. Organizations that perfect these skills respond quickly to new opportunities and changing market imperatives. Companies that don't will soon discover that online dollars are flowing elsewhere.

E-business and the Challenge of Network Security Point Solutions

On a superficial level, E-business follows a similar structure to the physical world. A company's goods and services become online transaction data. Vendors, suppliers and customers connect via the Internet and extranets rather than in person. Inventory becomes data moved between vendors, customers, suppliers and fulfillment houses. Revenue continues to flow in electronic form from the store to banking networks to the home office, and back again. As a result, E-businesses are dependent on an ISP and the Internet backbone itself for availability and convenience.

The rush to embrace E-business has been built primarily on browser-based encryption (SSL) and username/password authentication (.htaccess). Both methods are relatively easy to implement, and both come bundled as a basic component in web browsers and servers. Unfortunately, neither method provides much of an obstacle to attack and misuse. Adding to the confusion is the nature of TCP/IP communications. With 65,000 communications ports on any given network device, attackers have many avenues for subverting security infrastructure. Perfect security literally means simultaneously watching 65,000 doors and windows on a 24x7 basis, and never blinking.

According to traditional network security methodology, point solutions are sufficient to protect the E-business environment, provided a sufficient number of devices are deployed in a sufficient number of places. It is the department store equivalent of placing security guards in every department, tags on all the goods, sensors on all the doors to detect tags leaving the store improperly and surveillance cameras to watch all employees and visitors.

The business world learned long ago however, that risk can not be eliminated. Instead, it must be managed. At the department store, managers keep strict control of overstocks, mix styles to hedge against changing tastes, and use sales to move stale inventory. Static physical security is used where it makes practical, cost-effective sense, protecting the goods that cost the most to replace. Staff is held accountable for theft and misuse.

Most importantly, management sees security as an ongoing process. As new needs arise, the system adapts and grows to meet the changing circumstances. Part of the goal is to contain losses due to theft and vandalism, but a significant amount of the security is in place to protect the store's image.

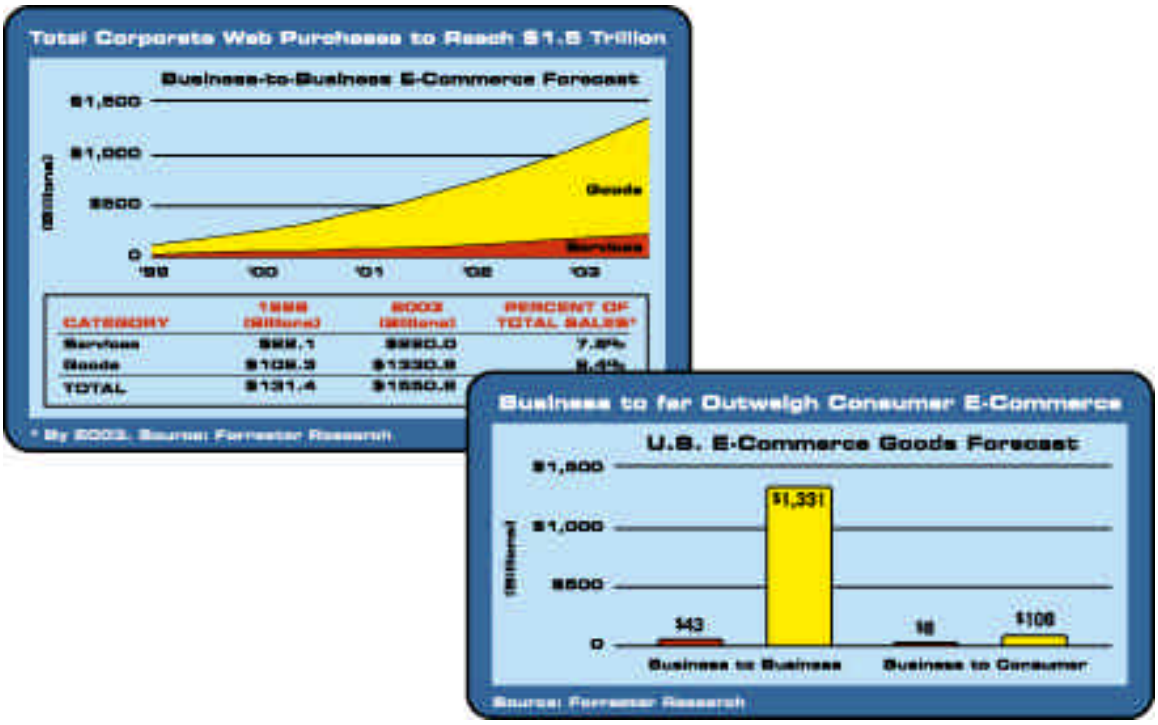
Firewalls, encryption servers, card keys, VPNs and similar technologies do not eliminate risk so much as they shift it from one part of the network to another. Poorly chosen passwords, borrowed card keys and misconfigured network devices easily foil access control and authentication. Encryption only protects data while in transit. It is still at risk before transmission and after it is arrived. Even worse, the encryption stream can be disrupted, corrupting traffic and causing expensive data integrity repairs.

Responsibility for protecting online assets tends to move over time from the people working with the data to IT staffs physically removed from the data creation process. If the network security staffs attempt to put all their resources on the network perimeter, they leave themselves exposed to internal misuse. If they wall off functional groups within an organization from each other, network performance degrades and end users perceive the barriers as unnecessary. Vigilance begins to wane as limited staff with limited resources can not cover all needs and eventualities. End users, frustrated with performance obstacles, begin to actively subvert the security safeguards. Breakdowns in protection become inevitable.

Maximizing Growth By Minimizing Online Risk

There are two basic types of risk involved in embracing E-business via open systems and networks. The first is the opportunity cost of not connecting openly with the rest of the online world. Online retailers reported $16.2 billion in revenues in 1999 *(BizRate).* This number is expected to increase to $40 billion in 2000 as ever-larger numbers of individuals and homeowners either connect to the Internet for the first time or upgrade to DSL, cable modem or other high-speed connections. Fully 1/6 of the world's population is expected to have Internet access by 2003 *(Cybercrime, Cyberterrorism, Cyberwarfare: Averting An Electronic Waterloo, CSIS Task Force, 1998).*

Business-to-business online commerce is an even greater success. Using a combination of Internet and direct extranet connections, companies racked up over $145 billion in sales in 1999 *(Gartner Group).* This new method of purchasing and receiving is popular for good reason. Online vending can significantly reduce the cost of sales by reducing the number of staff required to service a given account. Orders can route directly to fulfillment, cutting delivery times to the bare minimum. Finally, customers and partners can "self-help" with web-based databases, video help guides and similar online knowledge transfer technologies. And this number is expected to grow to $7.3 trillion by 2004.



The second and more obvious risk is the risk of damage when security point solutions fail. Penetrations at obvious web targets like the Pentagon and *The New York Times* grab headlines, but do little lasting damage. It is what is not publicized that is the most alarming. According to a recent FBI/CSI survey, more than 90 percent of respondents reported at least one security breach in 1999, with total verification losses topping $265 million. With partners and sometime competitors frequently combining forces on emerging target markets, rapid and secure sharing of time-critical information is crucial to making these shifting alliances successful. These joint ventures exist to take advantage of quickly evolving market dynamics. Without open systems and transparent access to each other's networks, they are impossible.

These well-publicized statistics can be frightening, but they obscure the real benefits of secure E-business. Properly constructed and protected online supply chains enhance revenue specifically because they minimize opportunities for attack and misuse. Open online supply chains allow organizations to aggressively streamline processes and improve efficiencies. Most importantly, these improvements create direct communications between producers and customers, increasing profit potential, customer satisfaction and brand loyalty.

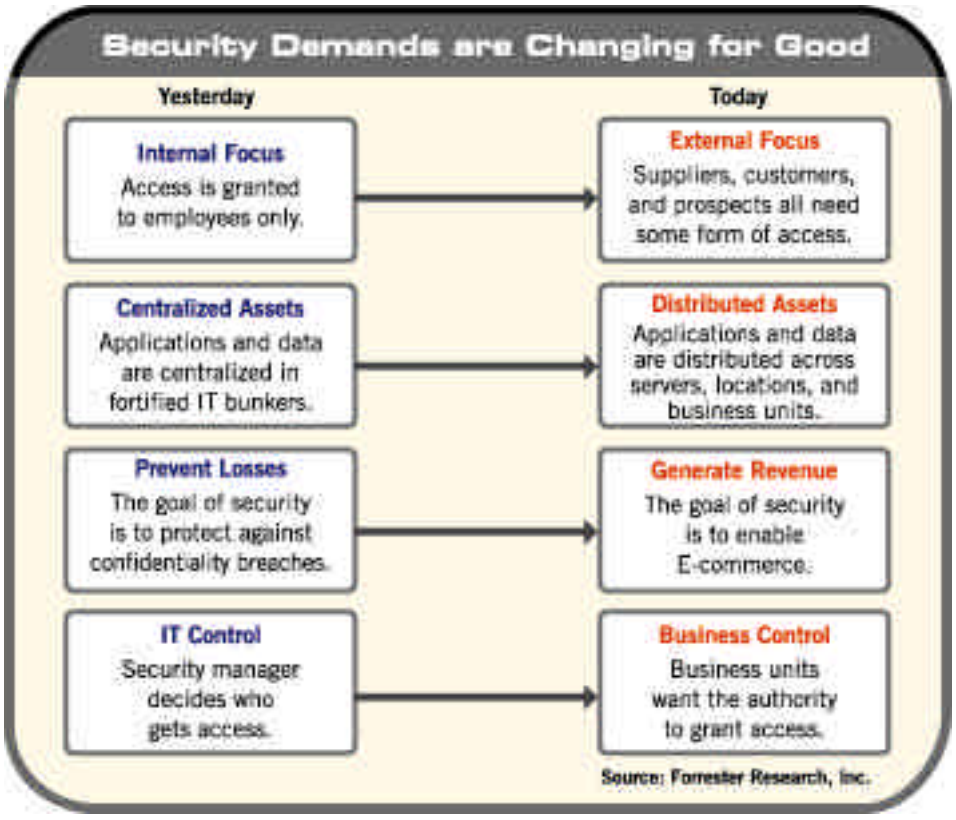
Secure E-business-The Online Opportunity Enabler

Organizations need a process that creates the transparent relationships necessary for the E-business supply chain to function. E-business requires a sophisticated model that encompasses storefront functions, manufacturing, inventory, warehousing, customer relationships, partnerships and banking services. By themselves, point solutions lack the flexibility to meet the E-business challenge. Businesses also need a risk management infrastructure to deliver these key pieces of the E-business puzzle.

Secure E-business therefore, allows organizations to rethink the way a business is run. Security evolves from risk management to opportunity management. The secure E-business process can even monitor buying patterns as well as streamline operations. Secure E-business helps organizations learn more about themselves and their target markets. And knowing more about customers and their buying habits is critical to online success.

Secure E-business enables online commerce by:

- Ensuring data availability, integrity and confidentiality
- Identifying vulnerabilities in hosts and networks that could lead to interruptions in service
- Creating secure, confidential channels for transferring business data up and down the entire online supply chain.



This simple, direct methodology simultaneously enhances online security while simplifying the process of opening hosts, networks and data stores to outside opportunities. Organizations using secure E-business solutions become more open, more flexible and better protected than their competitors. Buyer behavior analysis becomes an integral part of the E-business process. This agility leads to improved competitive posture and a rapid return on investment (ROI).

Secure E-business follows a simple set of principles:

- Understand your networks, and the business objectives they support. Some systems and information resources are more valuable than others, and not all of it needs to be protected equally.

- Develop a thorough and achievable security policy, implement it and update it at regular intervals. Use this process to streamline and automate operations and enhance cross-platform integration and distribution.

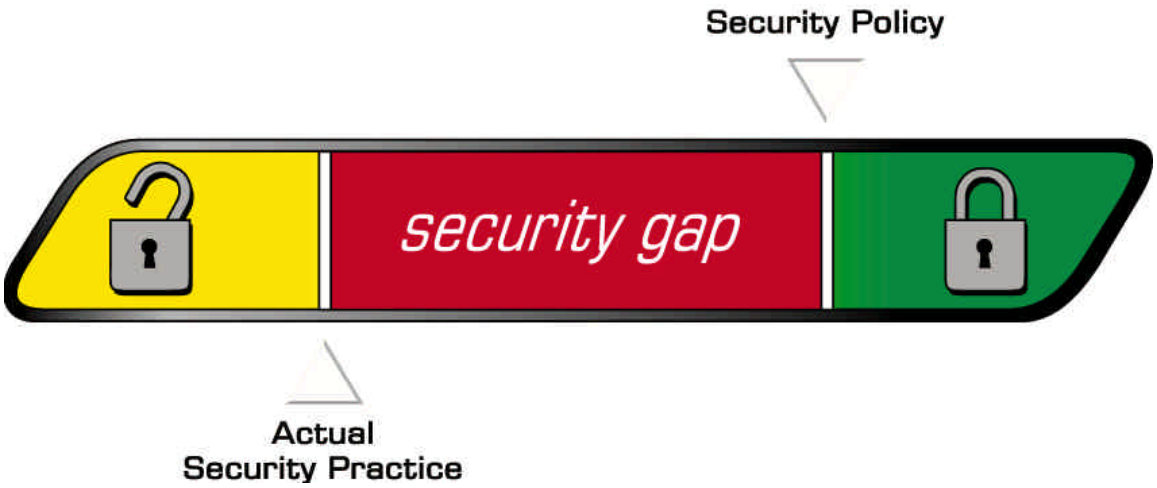
- Enhance point solutions such as firewalls, authentication and encryption with adaptive technology that maximizes effectiveness and helps prevent premature obsolescence.

- Purchase infrastructure products and assessment tools from different manufacturers. An independent source of assessment products is much more likely to provide an unbiased evaluation of overall E-business security performance.

- Consider outsourcing some or all security management operations. Doing so allows an organization to focus internal resources more directly on core business compentencies.

- Keep it simple. "Shun complexity. Set dirt-simple policies and use measures that are invisible to end-users. Obsess about ease-of-management to reduce the risk of misconfiguration" *(Turning Security On Its Head, Forrester Research, 1999).*

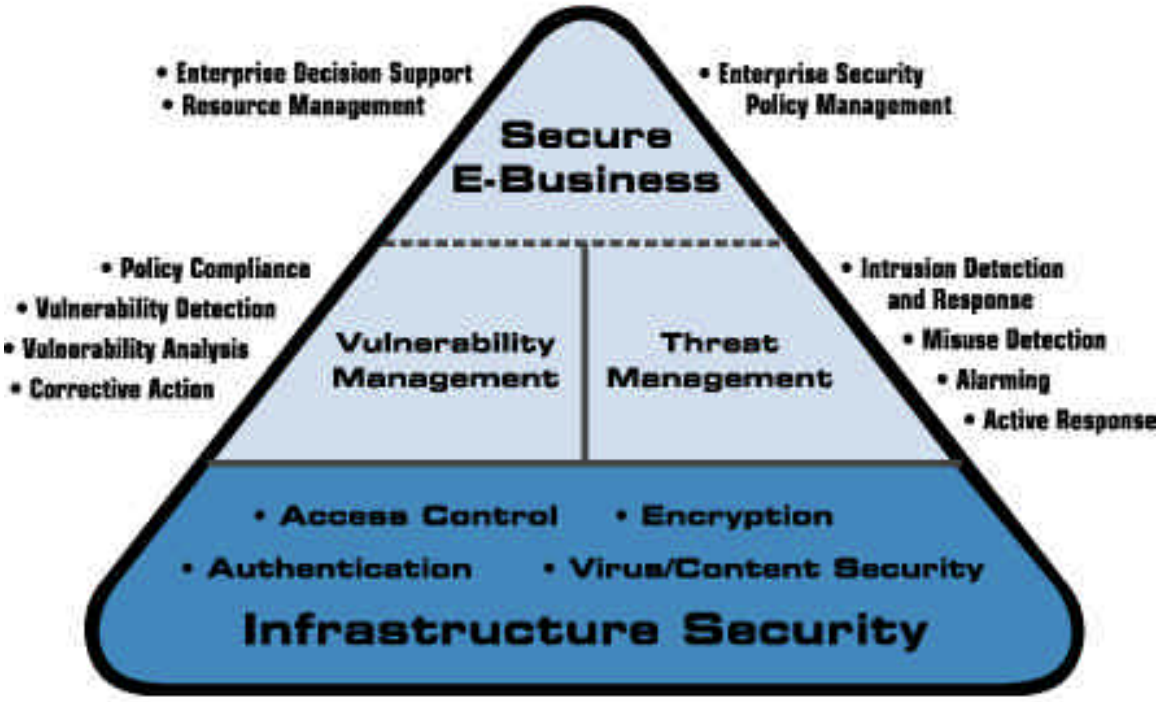
Many organizations already have some form of security policy. However, pressure from users demanding enhanced capabilities and limited staff resources often result in a significant gap between the policy and its actual implementation. This security gap is where a small oversight can lead to a huge problem. Secure E-business helps measure and control this gap.



Secure E-business consists of five closely related functions:

- Policy compliance and vulnerability managment
- Intrusion detection and reponse
- Enterprise Security Management and Decision Support
- Managed Security Services (outsourcing)
- Risk management and E-commerce insurance coverage

The next sections contain detailed descriptions of each secure E-business component. These processes interact with and support point solutions to monitor network security performance, detect vulnerabilities, attacks and misuse, and respond quickly to security violations to limit the effects of an attack and prevent future incursions. The end result is online supply chain transparency – the critical ingredient for E-business success.



Policy Compliance And Vulnerability Management

Network security policy has traditionally been a manual process. What starts as hardcopy documentation must somehow be translated into precise applications for network use, and distributed across the enterprise. It's a slow procedure, lacking the rapid response required in an open networking environment. Accountability is difficult to enforce.

Recent software advances accelerate policy development, including online distribution of policy implementation plans throughout an organization, with each plan customized for any given network device or application. Policy compliance begins by identifying what information is available online, and which part of that knowledge rates a specific level of

protection. When combined with a thorough catalogue of systems, networks, applications and databases, these results become the basis for creating a security policy – the blueprint by which an organization decides the level of protection for any online asset and the metrics by which the success or failures of that protection can be measured.

Once a policy has been defined, it needs to be distributed throughout the organization, both to staff in hardcopy format and to network devices as implementable applications and code. Some elements are equally enforceable for any network segment or device. For example, passwords should be eight characters long, combine letters, numbers and punctuation marks, and be changed every 60 days. Other aspects of the overall security policy may vary from department to department. For instance, what is and is not allowable for accounting computers may be significantly stricter than standards for an external web server.

Finally, both staff and network devices need to compare policy guidelines with performance in an actual production environment. Compliance assessment identifies more than potential security exposures – it also highlights aspects of security policy that may have become outdated or impractical. These regularly scheduled, cyclical policy audits ensure tight alignment between security policy and compliance, enabling networks to adapt to changing environments.

Once a security policy is in place, the next step is to systematically and regularly test hosts, networks, applications and databases for vulnerabilities. This step is directly analogous to internal audits in the physical world, measuring inventory and ensuring that the books are in order. Online weaknesses range from easily guessed or missing passwords, to misconfigured or unauthorized devices, to physical evidence of improper user activity. Once the online audit is complete, the results must be assessed as to relative risk. In other words, an unprotected and little used UDP port on a critical accounting system might be a severe risk, while leaving the same port unprotected on a web server outside the corporate firewall might be advisable as a useful channel for delivering streaming multimedia.

Some vulnerabilities can only be identified over the network. For example, the best way to verify that a web server is susceptible to a denial of service attack is by simulating that exploit across a network under controlled conditions. Other vulnerabilities must be detected directly on the host. Improper user, group or file permissions fall into this category. Finally, some vulnerabilities are particular to specific applications, such as database programming languages, javascript and macro utilities.

Specialized scanning software converts security policy into automated searches for these weaknesses. Target devices should include both network devices and the security infrastructure, including:

- Web servers
- File servers
- Application servers
- Intranet / extranet servers
- Firewalls
- Routers, bridges and hubs
- Modem banks and remote access gateways
- Databases
- Applications

The final step in Security Assessment is correcting any unacceptable security exposures uncovered in the assessment. A good Vulnerability Management system will contain a database of known weaknesses, step-by-step instructions for repairing them and online vendor resources for locating patches, updates and other needed software. After all relevant repairs have been made, individual systems should be marked with a digital fingerprint, making it obvious if that system has been improperly altered between scans and identifying that host or application as a strong candidate for further investigation.

Intrusion Detection and Response

Intrusion Detection and Response uses security policy as the basis for a sophisticated host- and network-based intrusion detection system. This technology serves as a savvy, experienced online security guard, anticipating possible misuse with a variety of response options. Host-and network-based intrusion detection products are usually sold as competing offerings from different vendors. However, integrated host and network systems are now available. This extra level of integration significantly enhances the overall effectiveness of any Threat Management solution.

Host-based intrusion detection monitors system, event, and security logs on Windows NT and syslog in Unix environments. When any of these files change, the intrusion detection system compares the new log entry with attack signatures – telltale patterns indicating an attack – to see if there is a match. If so, the system responds with administrator alerts, port and service closings, and other calls to action based on the severity of the incursion.

Host-based intrusion detection has grown to include other technologies, including detecting intrusions by checking key system files and executables via checksums at regular intervals for unexpected changes. The timeliness of the response becomes directly related to the frequency of the polling interval. Other products listen to port activity and alert administrators when specific ports are accessed. This type of detection brings an elementary level of network-based intrusion detection into the host-based environment.

Network-based intrusion detection analyzes raw network packets as the data source, utilizing a network adapter running in promiscuous mode to monitor and interpret all traffic in real-time as it travels across the network. Once an attack has been detected, the system's response module provides a variety of options to notify, alert and take action in response to the attack. These responses vary by product, but usually involve administrator notification, connection termination and/or session recording.

Host- and network-based intrusion detection are complementary rather than competing technologies. Network-based systems recognize and respond to attacks and misuse in real-time, making them ideal tools for stopping a network penetration before damage occurs, monitoring an attack in progress, and/or recording a secured set of logs for later forensic examination or possible prosecution. Host-based tools catch a variety of anomalies that network-based systems miss, and generally provide a lower initial cost of ownership. They are particularly useful in determining the mechanism of an attack, allowing administrators to quickly and automatically identify and reconfigure other parts of the network susceptible to a similar attack.

Managed Security Services

Experienced security management staff are hard to find and expensive to hire. The job requires constant vigilance and must account for each and every change in the network state. It is an enormous undertaking, and rarely within the core competency of any beginning or rapidly growing online business. The cost of a global, 24x7 in-house risk management solution, therefore, is out of reach for most E-businesses.

As a result, a rapidly increasing number of E-business ventures are turning to Managed Security Services (MSS) to ensure that online assets are being properly protected. MSS is similar to outsourced security, but it offers unique advantages that make it an ideal resource for E-business. Instead of separate vendors for security consulting services, firewalls, anti-virus, intrusion detection and other essential information security services, MSS combines these basic business necessities with thorough security assessments and comprehensive security lifecycle methodologies to deliver a complete, customized security management solution.

MSS delivers key advantages for both E-business start-ups and established enterprise players with massive online operations. Since all security operations take place at the vendor’s centralized Network Operations Center, clients don't have to worry about hardware, software, staff or operations. A management console application allows client oversight of all security operations, plus rapid response to changing network conditions.

MSS turns a potential security crisis into achievable security policy. It allows a company to start with basic security needs at low cost, then expand as the business grows. Since the security infrastructure is disbursed across the vendor’s entire managed services customer base, monthly security costs are minimized. Even so, each aspect of the enterprise can be cost-effectively secured against attack and misuse. There's no staff to maintain, and single vendor contact greatly simplifies support.

Risk Management and E-business Insurance Coverage

Perfect security management protection is both impossible and prohibitively expensive to achieve. As a result, a thorough Secure E-business should also include E-business insurance to bridge the gap between an achievable security management solution and truly comprehensive protection against business interruption losses. These E-business insurance policies can easily mean the difference between disaster and a quick recovery.

By combining security management solutions and E-business insurance coverage, a properly constructed risk management program provides the potential for significant cost savings while simultaneously accelerating online growth, reducing operational costs and reducing liability exposure. These programs determine levels of current risk, establish security policy and enforcement, and develop long range security best practices for each participating client's risk management needs.

Basic E-business insurance should cover media liability, theft of intellectual property, transaction coverage and indemnity against financial loss. In addition, adopting and following a risk management program should mitigate the cost of security management and E-commerce insurance with a monetary reduction in insurance rates. Clients

with relatively low risk exposure will receive the most cost efficient coverage. Clients considered to be at higher risk may still receive coverage, but at a higher rate.

Conclusion

When network resources are not available, organizations can not make money. Employee efficiency disappears until operating systems can be reinstalled, networks rebuilt and data integrity verified. Business opportunities move on to other organizations. Even limited or sporadic services outages can seriously damage the return on investment in a corporate portal, delaying profitability and limiting future growth.

E-business is based on the assumption that data integrity is intact and that online systems are always available when needed. Ensuring the availability of these key components is critical to online commercial success. When data is corrupt and systems are under attack, customers take their money elsewhere. In other words, no organization can deliver reliably available E-business systems if it is not actively monitoring the E-business security environment.

Information is the basis for competitive and strategic advantage. Therefore, managing the risk of exposure for online information assumes legal importance. Organizations that adhere to a strict regimen of policy management and compliance do more than improve corporate financial performance. They also reduce the chance of legal exposures and liabilities due to negligent protection of key corporate assets.

In a world where information is currency, secure E-business supply chains create new opportunities for streamlining business processes, creating a new, expanded customer base, and establishing the agility necessary to react rapidly to new markets and business models. It generates a rapid return on investment through improved data integrity, enhanced systems availability and intensified confidentiality across the online supply chain. The ongoing result is secure E-business creates a secure and confident environment for developing innovative online business opportunities. Secure E-business delivers increased revenue, maximized profitability and increased customer satisfaction through:

- Enhanced data integrity, availability and protection
- Increased employee productivity
- Extended security expertise
- Adaptive security management, measurement and metrics
- Lowered legal liability
- Improved and accelerated corporate portal return on investment

Organizations spend a great amount of time and effort developing partner, investor and consumer trust in the physical marketplace. Secure E-business brings that same level of assurance to online, interconnected economies. Organizations wishing to adopt E-business face a stark, obvious choice. Without secure E-business, they face limited adoption of Internet, intranet and extranet technologies and expensive, incomplete security implementations. With secure E-business, companies can aggressively move online with assurance, enhancing current market relationships while driving aggressively into tomorrow's markets and opportunities.

About Internet Security Systems

Internet Security Systems (ISS) is a leading global provider of security management solutions for the Internet. By providing industry-leading SAFEsuite security software, remote managed security services, and strategic consulting and education offerings, ISS is a trusted security provider to its customers, protecting digital assets and ensuring safe and uninterrupted e- business. ISS' security management solutions protect more than 6,000 customers worldwide including 21 of the 25 largest U.S. commercial banks, 10 of the largest telecommunications companies and over 35 government agencies. Founded in 1994, ISS is headquartered in Atlanta, GA, with additional offices throughout North America and international operations in Asia, Australia, Europe, Latin America and the Middle East. For more information, visit the Internet Security Systems web site at www.iss.net or call 888-901-7477