

WHITE PAPER

Enterprise Security: Changing Needs, Evolving Response

Sponsored by: VeriSign

Christian A. Christiansen Charles J. Kolodgy
Roseann Day
April 2003

OVERVIEW

As threat environments grow more virulent, economic pressures increase, and the geopolitical situation destabilizes, enterprise IT security constantly changes in scope, importance, and implementation. To counter these pressures, IT managers are deploying increasingly reliable and more maintainable security solutions to help fight the rising tide of threats and internal economic justifications.

This white paper explores some of the most pressing demands security executives face, their current deployment plans, and their key security needs going forward. It also presents VeriSign's strategy and mission to support these needs.

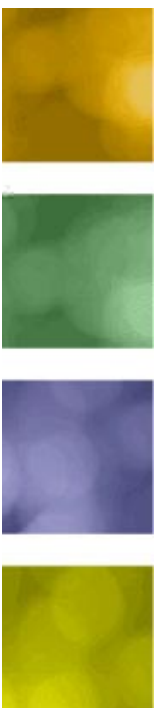
METHODOLOGY

IDC conducts ongoing interviews with technology and business professionals on relevant information and communication technology (ICT) issues. The survey results and the analysis that follow are derived from one of IDC's three *Enterprise Technology Trends Surveys (ETT Surveys)* that are developed and administered every year. The current survey was conducted between mid-March and mid-May 2002 and has a respondent base of 883 U.S. and Canadian companies. Comprehensive analysis from these demand-side surveys is published for three company size segments, defined as small (10–99 employees), medium-sized (100–999 employees), and large (1,000+ employees).

The sample base is stratified by company size and weighted to reflect the North American ICT marketplace. Sample size may vary for any one variable, depending on participation. The study focuses exclusively on commercial markets.

Respondents, who are interviewed as end users of technology, were screened and qualified based on these criteria as well as on their decision-making authority and the scope of ICT activity within their organizations. The survey data was collected through a programmed questionnaire administered over the Web. We also screened the respondents via telephone to ensure that they met the sample target qualifications. This online method allows for detailed question sets, complex skip patterns, and real-time calculations, which in turn assist respondents in answering questions involving numbers and percentages. At the same time, the telephone screening provides a high level of control over which companies and respondents qualify.

Note: All numbers in this document may not be exact due to rounding.



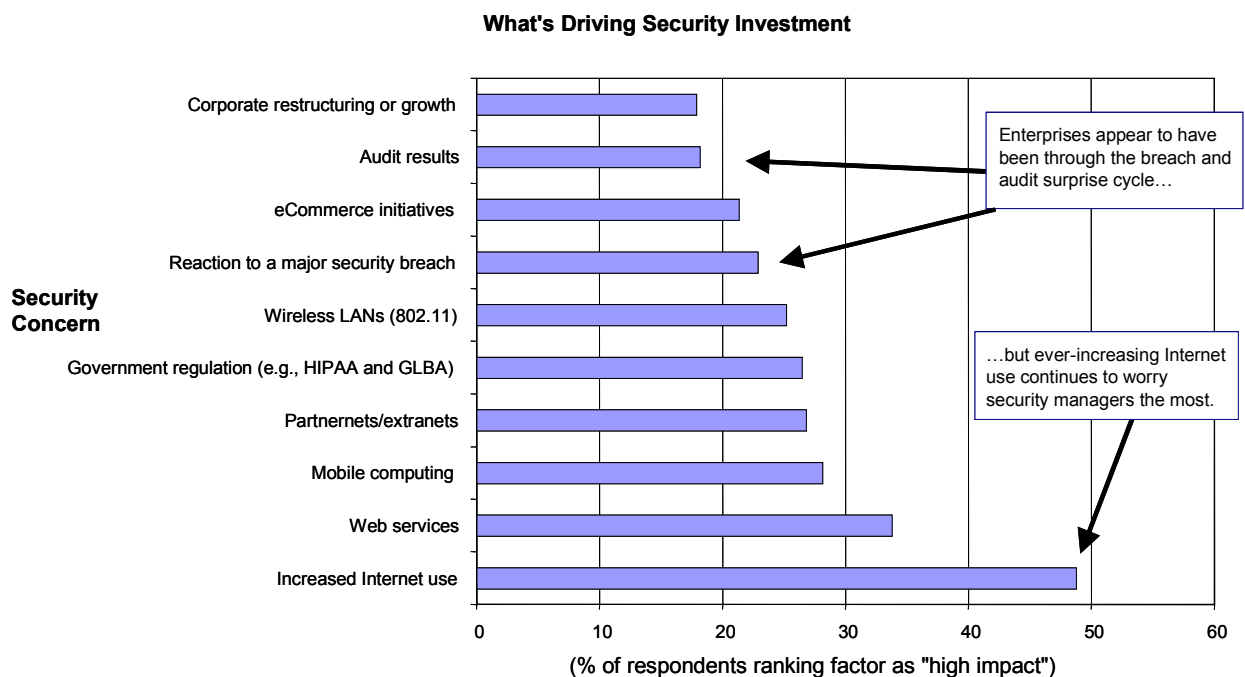
TOO MANY PRESSURES, TOO LITTLE TIME:
CRITICAL SECURITY NEEDS TODAY

While time and experience have turned enterprise security managers into veterans in dealing with common threats, many common problems, albeit multiplied, continue to plague them.

Based on data from an IDC survey conducted in late 2002, Figure 1 shows the drivers of security investments.

FIGURE 1

ENTERPRISE SECURITY PRIORITIES



Source: IDC's 2002 Enterprise Technology Trends Survey

INCREASED INTERNET USE

Increased Internet use was most frequently rated as having a high impact on security measures deployed at a company. Within the survey, 53.4% of respondents gave this event a "high impact" rating, ranking it as the highest-impact item driving their use of security technologies.

Inevitably, this increasing usage is reflected throughout the survey's results because the issue goes beyond escalating usage. Employees are not just looking at increasing volumes of HTML content. They are now connecting to broadband services that enable them to leave their computers constantly attached to the Internet. In part, this "always on" state is desirable because employees want to access online applications and get privileged access to corporate LANs via virtual private networks (VPNs). At the same time, enterprise employees and customers want access to even more

advanced Web applications such as ecommerce and mobile computing. Respondents cited these demands as the factors having a high impact on security investment. Interestingly, all these factors blur the line between security products and services.

REACTION TO MAJOR SECURITY BREACH AT YOUR COMPANY

Roughly one-third (34.2%) of the respondents perceived "reaction to a major security breach at your company" to be a high-impact factor. The potential for breaches from unseen hackers still worries enterprises considerably, but this concern joins a host of base-level concerns about relying on the public TCP/IP network for more and more core business activities.

Responding to security breaches takes a toll in multiple dimensions. First, support staff needs to be available 24 x 7 to respond and take proactive steps. Often, an external issue, whether it is political or business in nature, may require unusually high levels of staffing for specific time periods. Businesses often find it expensive and difficult to obtain the right staffing for that role. Next, the flow of business operations and the integrity of enterprise IT resources are susceptible to disruption. Both can hit the bottom line very hard. In some industries, particularly healthcare and finance, breaches can put executives at risk for fines and negative publicity. For executives concerned about a long list of issues, just contemplating the impact of such breaches can cause sleepless nights.

WEB SERVICES AND INTEGRATION

The world of partnernets, extranets, and integrated cross-enterprise data sharing continues to demand attention. Web services — an emerging platform for interbusiness, hands-free communication — takes today's stage as a leading driver of security concern. Thirty eight percent of the large enterprises surveyed in our annual security study identified Web services as "high impact" — thus, it is the second ranking driver for security spending. The ever-present task of managing provisioning and authentication for valid partners, suppliers, and customers compounds a challenging scenario.

GOVERNMENT REGULATIONS

Surprisingly, only 20% of the respondents perceived "government regulations" as having a high impact on the deployment of security measures. IDC believes government regulations impact banking and other credit institutions and healthcare services organizations significantly more frequently than other industry sectors. Given that government regulations are primarily associated with specific verticals, this would explain the low number of "high impact" responses across the broader survey sample.

Despite these results, we believe that the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and other regulations are placing considerable, serious pressure on selected verticals. In another IDC survey, more than 80% of both the healthcare and banking verticals indicated that these regulations are driving security investment and direction within their industries. These regulations also drive focused security and privacy planning and implementation at these enterprises. Growing concerns over increasing privacy regulations and IT protection while ensuring corporate compliance are likely to keep the pressures on.

SECURITY IMPLEMENTATION: WHAT WORKS, WHAT DOESN'T

Against this backdrop of escalating requirements, enterprises face thinning resources. Cost concerns balance the overall security implementation space.

BASIC SECURITY SINKS INTO THE NETWORK, FOCUSED SECURITY STAYS HIGH

"Old threats don't die; they just keep coming back at you" goes the saying about the cumulative nature of security threats. Standard protocol threats and viruses remain extant, while new threats and problems emerge. However, security vendors are continuing to streamline solutions to enable enterprises to protect against these known threats in a simpler and faster manner. Cisco and other network appliance vendors offer filtration capabilities tightly integrated into the router and switch environment.

However, the area of focus for enterprise security staff moves higher as basic security is subsumed into the infrastructure. For example, application access and authorization as well as tiered controls are becoming focal points. Effective application security controls require new solutions, integration, and training.

COST, COST, AND COST

The worldwide global economic downturn heightens perennial concerns over longer-term costs of security solutions and their ongoing maintenance. The need for effective, hands-free integration and maintenance of key security products, coupled with the need for consolidated central management, demands a new approach. Solution integration, native access, and central console control become essential.

Ease of management and support come first. Larger players with scale and range hold the upper hand over point solution providers in supplying enterprises with what they require.

SECURITY LEVELS AND ALLOCATIONS

Not all resources are equally valuable. Therefore, not all applications, data, locations, or subnets require the highest possible security. As enterprises gain the ability to discriminate applications, data, users, and transaction types, security associated with those components will become increasingly pliable and adaptable. VPN, for example, plays widely, but not ubiquitously. More data and messages — but not all — may require encryption. Better edge filtration gets deployed, but not to every edge. Enterprises are evolving their security implementations to reflect differential handling of assets. Security "best practice" approaches will address ecommerce, applications, network infrastructure, and content in similar fashion. Covering the entire domain at some level becomes critical because in today's environment leaving any one domain open can compromise the entire environment. The situation compares with that of the homeowner who locks the front door but leaves the key under the doormat.

TACTICAL ISSUES: THE FOUR DEADLY "Ps" OF ENTERPRISE SECURITY

Actual tactics determine how effective security technology can be. The following four areas are particularly challenging to implement correctly.

PATCHES

Vendors rely on patches and updates as the mechanisms for supplying essential improvements and fixes. However, enterprises continually struggle to remain current

with the ever-increasing number of required patches and upgrades. Patches cover systems, applications, and security at all levels of the infrastructure (i.e., desktop, server, and network). IT professionals often receive little help from vendors as to the correct prioritization of patches and face legitimate concerns about how to test patches in closed environments before applying them to production environments.

POLICY

The process of creating and deploying good policy is difficult in complex, changing environments. Too often security policies are limited or nonexistent. After creation, they are difficult to monitor, enforce, audit, or revise. Poor or untested procedures further weaken even the best-drafted policies.

PERSONNEL

Accountability is essential for good security. Too often no named individual(s) are singularly responsible for corporate security architecture, implementation, and policy revision. The ideal is a "single throat to choke" for failed security audits or when breaches occur.

PROTECTION

Consistency counts, too. Forgotten, ignored, or poorly maintained security environments make even the best technologies ineffective. Thus, firewalls need proper configuration, intrusion detection systems (IDS) must be monitored and tuned, and antivirus (AV) updated.

STRATEGIC ISSUES: RECONCILING RISK, TRUST, THREATS, AND COSTS

IS SECURITY A SERVICE OR A PRODUCT?

Customers who are accustomed to the rigor and discipline of other IT environments often find security a Sisyphean task. According to the Greek myth, Sisyphus was condemned to the underworld, where he was required to constantly roll an enormous rock up a hill only to always lose control shortly before completing the task. Thus, he was forced to start from the beginning.

Just like the toils of Sisyphus, security is a never-ending task. Because of the evolving threat ecosystem (amateur hackers, disgruntled insiders, and professional criminal crackers and espionage groups), security requires constant vigilance. This threat environment fosters rapid obsolescence of many security products. Moreover, IT personnel must constantly balance their time between fulfilling their IT chores and training on the latest security threats and technologies. In many companies, this balancing act is considered a costly sideshow by senior management.

Given this unpleasant situation, enterprises of all sizes are considering security a service. Senior management is increasingly reluctant to fund ever-increasing budgets for security products and training. Even when senior management can train its IT people in security practices and methods, these highly trained IT employees often leave for better-paying jobs at other companies. Moreover, company owners don't want to fund the development of an expertise that is not directly applicable to revenue generation or increased profitability. Given this situation, many companies are increasingly questioning the large budgets to develop a core expertise in security. However, security is still the number one concern of all IT organizations, and even senior management regards security spending as mandatory.

This situation creates a conundrum around improving security while maintaining IT personnel and budgets focused on corporate priorities. Currently, IT provides security services to its customers by purchasing products. However, some companies are starting to realize that a dual services approach can reduce security product purchases for networks, applications, ecommerce, and even content security. Security services in all these areas can mesh with customers' existing security infrastructures. Moreover, using security services permits companies to extend security support for new customer requirements (e.g., ebusiness, remote access, mobile computing, remote office/branch office, and partnernets). By using services for these extensions, companies can (1.) avoid expending additional, limited internal IT resources; (2.) defray the cost of training internal personnel to develop new areas of security expertise; and (3.) leverage the managed security firms' existing expertise to ensure the security of initial implementations .

APPLICATIONS SECURITY, IDENTITY MANAGEMENT, AND WEB SERVICES

A web of threats impacts applications security, identity management, and Web services. Hackers are discovering Web applications and databases as the paths of least resistance and greatest profit for misuse of networked assets. Improving application-layer security and tightening identity management will be key to the widespread adoption of Web services.

Application security currently focuses on vulnerability testing of software code. Instead of fixing security bugs in applications code after release, security vendors will catch some security problems (e.g., buffer overflows) prior to release. Increasingly, vendors and in-house programmers will bake security into their code during development instead of smearing it on later after the application is in production.

There is another ingredient in the applications security cookbook that will assume greater importance. As enterprise software vendors begin addressing customer requirements for better identity management, they will partner with authentication, authorization, administration, and provisioning vendors to build identity management into their products. In turn, identity management will provide the critical security foundation for Web services. IDC believes that Web services implementation will require tight authentication and authorization of users, processes, applications, and network devices.

As our survey research shows, Web services security is the third major driver of security purchases. IDC defines Web services as an application interoperation architecture in which self-describing components dynamically connect to form a distributed application. These services use standard protocols for content description and messaging, including but not limited to XML, WSDL, and SOAP. Web services protocols allow application-to-application and machine-to-machine, "hands-free" business interaction.

The prominence of the security concern with Web services is truly surprising given that only a few years ago the majority of IT organizations were not even planning to deploy them.

This market is actually a "superset" because it draws from many markets (e.g., encryption, public key infrastructure, authentication, firewall, and VPNs). For customers, the benefit is the ability to connect all their applications, data, and networks together. This extension holds the promise of improved infrastructure efficiency, greater customer access, and improved employee efficiency with relatively moderate software and services expenditures. In the current economic situation, this improved efficiency could yield significant cost savings and return on investment (ROI).

The genesis for Web services security already exists in XML encryption, XML signatures, authorization, and authentication. Moreover, the standards bodies (WS-I and OASIS) are incorporating XML security technologies into identity management frameworks. We believe that identity management in turn will provide the critical authentication and authorization infrastructure for Web services security.

ECOMMERCE BUILDS ON WEB SERVICES

Current technologies and managed services consist of access management, public key infrastructure for robust authentication, and secure messaging. We see the previously discussed Web services incorporating and integrating all these elements for seamless and secure customer experiences with ecommerce sites.

NETWORK SECURITY GETS POLICY ENFORCED CLIENT SECURITY

Desktop security initially focused on wireline access; however, increasing comprehensive desktop security will expand as corporations realize that policy enforced client security (PECS) can bridge the wired and wireless worlds with a single corporate security policy. PECS will combine authentication, authorization, policy, firewalling, antivirus, and security patch management. It will also increasingly apply to server-passed solutions.

Available from a broad range of vendors, PECS will gain momentum as enterprises become more sensitive to the risks inherent in increased dependence on Web services.

PUBLIC POLICY AFFECTS ENTERPRISE SECURITY STRATEGIES

Enterprises cannot set security policy without paying heed to public policy, which is currently receiving an extraordinary level of attention. Homeland defense spending will not boom until fiscal year 2004 or calendar year 2005. Even then a significant share of the tens of billions of dollars will go to physical security (e.g., gates, guns, guards, and dogs) and explosive detection equipment. Government IT security spending will underperform expectations. Moreover, vendors will need to partner with major defense contractors/systems integrators (e.g., Northrop Grumman, Lockheed, Raytheon, SAIC, CSC, and Unisys) to successfully sell into government accounts.

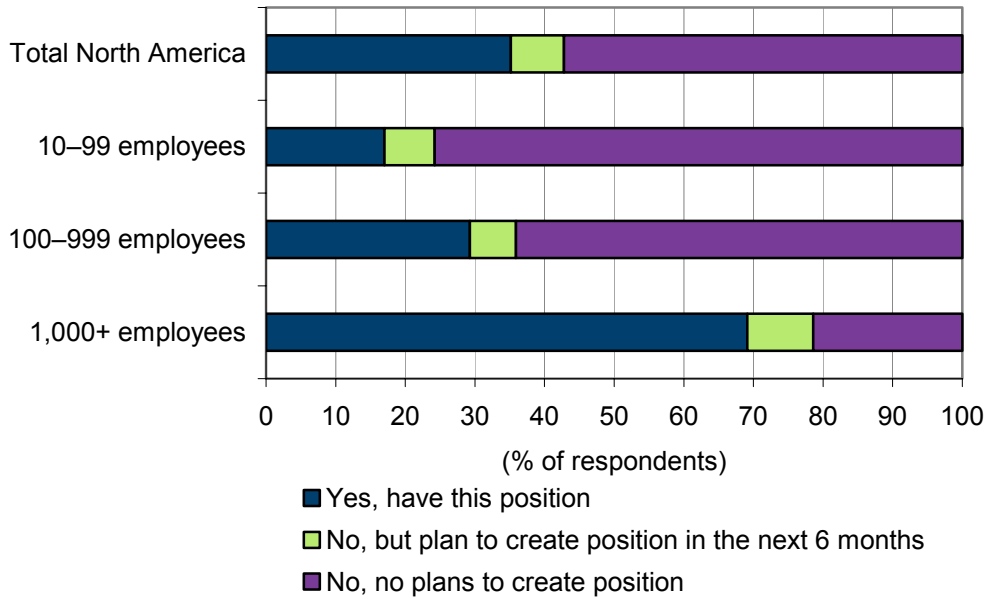
Public policy also dictates more attention to the handling of personal data. Privacy becomes legally sanctioned as GLBA, HIPAA, and Sarbanes-Oxley bring privacy spending to roughly 10–15% of the total security market.

CORPORATE SECURITY POLICY IS ENFORCED BY CXO-LEVEL SENIOR MANAGEMENT

It is extremely difficult to reach consensus on, gain business units' buy-in for, enforce, and periodically refresh security policy. We expect these challenging tasks will encourage the development of policy creation, enforcement, and management tools. Many of these tools will offer templates for HIPAA and GLBA as well as for handling general security audits. Corporations are also trying to get a handle on their security policies by creating a chief security officer (CSO) position. CSOs will oversee all aspects of corporate security, including policy creation and enforcement. Figure 2 shows that more than 60% of larger enterprises surveyed stated that they had established the CSO position.

FIGURE 2

CHIEF SECURITY OFFICER ASCENDANCY BY COMPANY SIZE



Source: IDC's 2002 Enterprise Technology Trends Survey

SECURITY MUST DELIVER ON ROI

Good security is more than expensive liability insurance. It can be a business enabler. Good security keeps out the bad guys, but, just as important, it lets in the good guys — efficiently. Corporate managers will continue to insist that security spending show an ROI. Until strong data on ROI is widely available, many corporate networks will remain riddled with security holes. Savvy IT managers are starting to realize that without appropriate security, a breach is more likely to occur in the current environment, which could prove much more costly than any investments made in security.

AUTHENTICATION AND AUTHORIZATION FOR MOBILE COMPUTING BECOME MAJOR SECURITY CHALLENGES

Broadband's increasing proliferation is highlighting the growing awareness of security need. Personal firewall (PFW) vendors have strongly benefited from this increased awareness. Given that consumer broadband penetration continues to expand worldwide, we believe consumer demand will remain high for PFW software and firewalls embedded into low-end routers. We also expect rising demand for consumer IDS products. All major PFWs incorporate some IDS functionality.

Corporations are also recognizing that their remote access policies must deal with consumers' household networks and diverse family members who use these networks. In addition, the line between consumer-based and corporate remote access is growing increasingly blurry. As a result of this crossover, we expect increased growth of software-based distributed firewalls (DFWs). The primary goal is to enforce corporate security regardless of the employee's location. Because so many remote users are installing their own home networks, we believe that DFW and remote access vendors will build in capabilities that allow corporate IT to ensure that only the

employee on this multiuser home network accesses his or her sensitive business traffic. After all, most teenagers despise security, and an even worse scenario would involve their undesired presence in their parents' corporate access policies and procedures. These situations are ever more alarming. Given the multitude of sophisticated users on home networks, we expect more intelligent routers and wireless access points with DFW, point-to-point VPN, IDS, supply chain management (SCM), access management (locally and/or remotely administered), and hardware authentication support (tokens, smart cards, and biometrics).

ECOMMERCE CUSTOMERS AWAKEN TO SECURITY CONSCIOUSNESS

Consumers increasingly understand that security is a necessity. Identity theft, credit card fraud, broadband associated vulnerabilities, and wireless traffic sniffing are all contributing to a certain level of ecommerce paranoia.

Product purchases of AV software remain surprisingly strong. However, we believe that consumers are becoming more aware that security is a subscription service that must be maintained rather than a one-time product purchase. Consumers are also beginning to realize that AV alone does not provide enough security. Broadband connections must have firewalls, or they will get hacked.

Because most consumers will want to suffer only a small role in security management, they will increasingly turn to service providers (SPs). SPs already supply some FW, AV, Web filtering, email scanning, and spam control, but as free or low-cost monthly services. We expect the availability of low-cost security appliances that are built on top of routers and wireless access points will accelerate this trend.

STRONG CREDENTIALS AND TIGHT IDENTIFICATION FOR EMPLOYEES, CUSTOMERS, SUPPLIERS, OR PARTNERS

Identity management is a major issue for businesses and governments alike. The very open and anonymous nature of the Web is antithetical to positive identification. IDC believes client certificates, like single sign-on, will become a key component in identity management solutions and offer key benefits, including:

- ☒ **Authentication.** Verification that the user is who he or she claims to be.
- ☒ **Confidentiality.** Ensuring that the data is not revealed or disclosed to unauthorized people.
- ☒ **Integrity.** Protection against data being improperly modified or duplicated.
- ☒ **Nonrepudiation.** Preventing a party involved in a transaction from later denying that he or she actually participated in the transaction.

While client certificate usage lags that of server certificates, various emerging business applications, including secure messaging, wireless LANs, Web access, form signing, and VPNs, are expanding the use of client certificates.

VERISIGN

VeriSign is developing a comprehensive solution set in keeping with its mission of providing, cost-effective security services, consulting, and other professional services. The company has built a highly scalable, 24 x 7 infrastructure to provide critical services for digital commerce and communications. For instance, VeriSign runs the root DNS servers for the .com, .net and .org domains, processing more than *8 billion* DNS lookup transactions daily. By leveraging this shared infrastructure, VeriSign is able to provide security solutions very cost-effectively to enterprises of all sizes.

Furthermore, VeriSign also uses its infrastructure to provide Internet health monitoring in addition to monitoring the enterprise and its partners' environments. Today VeriSign offers the following services for security management:

- ☒ **Network/infrastructure security.** To ensure enterprise security for customers' LANs, VPNs, remote access, and wireless LANs, VeriSign offers managed security services that can reduce IT's burden and risk. These services encompass firewalls, IDS, VPNs, and authentication. Because misconfiguration is the leading cause of security failure and patch management in large, distributed environments is just a nasty nightmare, relying on a managed service can partially shift the risk from IT onto the service provider. As a pure-play managed security service provider that monitors and manages security devices for various customers, VeriSign can take advantage of its wide view of the network. That is, it can leverage early experience on vulnerabilities and potential threats from across its entire customer base. VeriSign offers these customers a level of proactive protection in this way.
- ☒ **Application security.** With perimeters and differences between internal and external users becoming increasingly gray, controlling applications' access is another nightmare. Various regulations such as HIPAA and GLBA also require strong authentication for users accessing applications and databases. Moreover, more and more users are connecting remotely. Considering this situation, enterprises see a critical need to secure access to applications as well as machine-to-machine access for Web services. VeriSign offers a complete suite of identity management and authentication services to protect and secure access to critical applications. The rise of Web services where information is increasingly exchanged from process to process will only increase the need in this area.
- ☒ **eCommerce security.** eCommerce is already tricky and prone to fraud because weak transaction rates and customer convenience crippled much needed authorization and authentication. VeriSign uses strong authentication and authorization to protect companies' ecommerce transactions by providing solutions for both sides of the transaction — the buyer and the seller. Currently, VeriSign protects more than 400,000 Web servers (sites). More important, it baked this level of security into applications-level identity verifications and payment systems so customers do not have to assemble their own solutions from piece parts. VeriSign's business authentication process ensures the Web site's identity with a reliable government-backed record of the business' existence. In addition to these ecommerce security capabilities, VeriSign also offers payment gateways, which process a significant volume of ecommerce transactions today.
- ☒ **Fraud and risk management.** VeriSign provides a flexible and comprehensive suite of fraud and risk management services to help large merchants proactively manage business risk. For many large merchants, fraud management involves controlling network, account, transaction, and administrative security domains. Because financial institutions within the payments industry hold the merchant financially and legally responsible for fraud, both online and offline, increased losses can become financially devastating for companies of any size. VeriSign has designed its consumer authentication, account monitoring, buyer authentication, and fraud protection services to provide high-grade risk control without interrupting the business processes of merchants or the buying processes of consumers.

VeriSign offers both services and technologies that customers can customize for varying fraud detection requirements. The company ties its fraud and risk management services to its secure payment gateway solutions — providing transaction screening and account monitoring for a wide range of credit and Automated Clearing House payment approaches.

- ☒ **Content security.** Enterprises are becoming increasingly concerned about the information content they communicate via email, Web, and ecommerce. They run a liability risk if the content itself violates rules or if they do not adequately secure its private delivery. For example, HIPAA regulations place considerable pressure on healthcare institutions to protect content. VeriSign deploys both managed services and technologies to help enterprises tighten controls on the distribution of sensitive data and protected content that flows outside the enterprise.

With its industry knowledge and experience and substantial physical infrastructure, VeriSign can play an important role in the greater emergence of secure internal and external applications and IT infrastructure.

CHALLENGES

Enterprises face significant security challenges. Technology alone cannot solve all the challenges. To help correctly position what it can do for users, VeriSign must also help educate them. IDC believes that VeriSign, as well as other security vendors, and its aggregate customers must come to a common understanding around the following issues:

- ☒ Good security is based on an enterprise's common agreement on a security policy. Policy development is largely based on agreement and understanding between senior management, IT, business unit leadership, employees, contractors, consultants, suppliers, distributors, resellers, and customers. If all the elements in this ecosystem do not agree, security holes will continue to exist.
- ☒ Best practices means that this "common ground" must be hammered out in a series of tedious and often confrontational meetings. The results of these meetings must be translated into security rules and procedures. Although technology can help with this step, continued reeducation requires manual intervention, thus reducing the overall value of the policies. While VeriSign's managed security, authentication, and authorization services are critical parts of this process, making these functions more seamless and less apparent to the end user is the challenge and opportunity. As a security utility provider, VeriSign can play a significant role in helping enterprises establish these security policies. This transparency can yield reductions in employees' mismanagement of their personal security (e.g., remote access and VPN) while improving the security efficiency of IT.

CONCLUSION

Today's complex business and technical environments combine to create a host of technical and security challenges for the IT executive. Attempting to launch new Web services and electronic initiatives can be daunting enough without having to stretch limited IT resources to develop security solutions to protect these Web initiatives. VeriSign's security solutions and managed services offer a cost-effective approach that allows businesses to focus on the complexity of their core business competencies at the same time that they address security best practices.

COPYRIGHT NOTICE

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2003 IDC. Reproduction without written permission is completely forbidden.