



Strengthening End-to-End eBusiness Security and Privacy

An IDC Executive Brief (#24)

Adapted from: Information Security Services Worldwide Market Forecast and Analysis, 1999–2004, IDC #[23166](#), November 2000

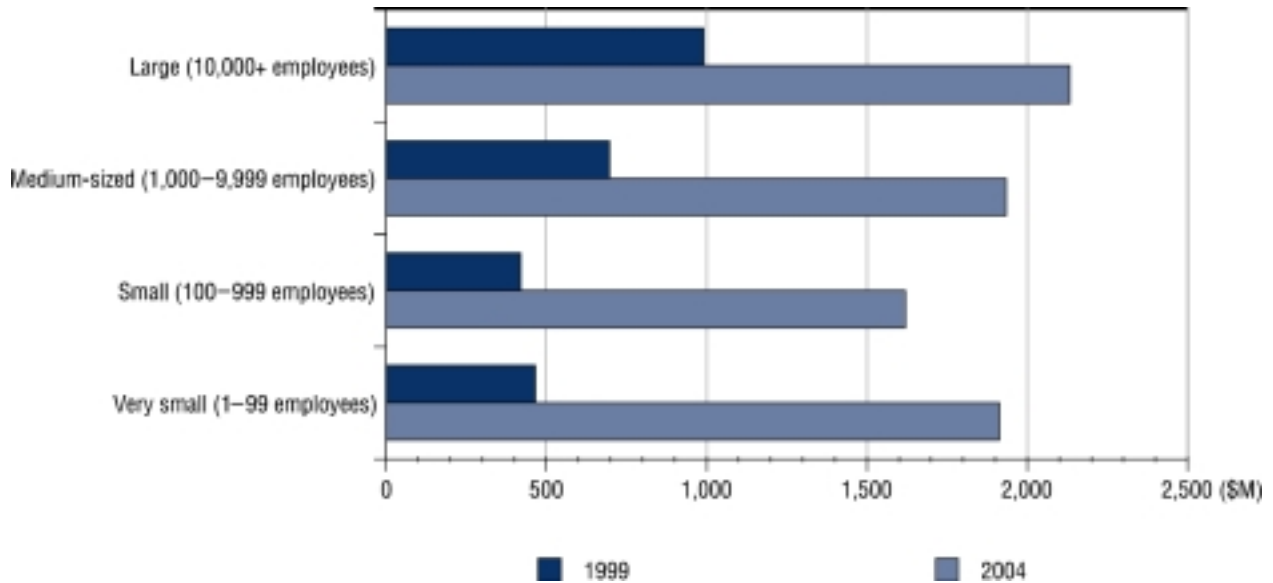
Creating a high-security, high-performance ebusiness infrastructure demands close coordination of both technical and management policies and procedures. The time and costs associated with monitoring all external connections, internal activities, and vulnerabilities are overwhelming IS departments and corporate executives alike. As a result, many corporations must rethink the overall network strategy and its effectiveness in enabling enterprisewide business objectives.

Furthermore, ebusiness security is evolving from the old notion of turning the enterprise into an information fortress to a new, more comprehensive model of privacy and trusted ebusiness.

IDC predicts the U.S. information security services market will grow from \$2.8 billion in 1999 to over \$8.2 billion in 2004, a compound annual growth rate of nearly 25%. Information security services are the activities and skills associated with planning, implementing, and managing highly secure networks.

The growing importance of ebusiness is influencing companies of all sizes to invest heavily in security services, as Figure 1 shows.

Figure 1
U.S. Information Security Services Expenditures by Company Size, 1999 and 2004



Source: IDC, 2000

When implementing a new security solution, an enterprise must have many goals in mind. These include:

- **Mitigating and managing security risks.** This is the traditional role of security — keeping intruders out and keeping information safe — and must be maintained.
- **Privacy — protecting personal and corporate information.** This is one of the biggest changes in the security market: Greater demands to share information with customers and partners is putting new stress on companies to prevent that information from falling into the wrong hands. Data control and management is a critical issue for corporations. Customer information in customer relationship management (CRM) systems is a valuable asset and must be protected.
- **Quickly deploying secure ebusiness initiatives.** In the new economy, time is always of the essence. Security solutions must keep time-to-market issues in mind, allowing the ebusiness environment to be modified on the fly without compromising security.
- **Reducing ongoing costs of managing and administering security.** Return on investment (ROI) is always a key goal, and it's a large driver behind outsourcing security. Companies that outsource security administration can

always be up to date with the latest solutions, without buying new products or hiring new expertise.

Security Requirements for eBusiness

The security infrastructure needs to have the following basic capabilities:

- **Identification/authentication.** This is the first step of any security and privacy process: being able to tell who users are. Having a security infrastructure that can do this quickly and accurately is necessary for creating a good quality of experience for customers and partners. Enterprises also need to be able to quickly modify user lists, which involves assigning users to roles/groups, thereby determining their level of access.
- **Authorization.** Once the system determines who users are — and that they are who they say they are — it must provide the correct levels of access to different applications and stores of information.
- **Asset protection.** The system must keep information confidential and private. This has become more difficult in the modern ebusiness environment, where information isn't just sitting in a database but traveling across multiple, often untrusted, networks. The security solution needs to ensure that information isn't stolen or changed in transit.
- **Accountability.** This is the ability to keep track of who has done what with what data. If security breaches or misuse of information occurs, this makes it easier to track down possible culprits. eBusiness solutions also need to ensure that participants in transactions are accountable as well.
- **Administration.** This involves defining security policies and implementing them across the enterprise infrastructure, consistently across different platforms and networks.
- **Assurance.** This demands mechanisms that show the security solutions are working, through methods such as proactive detection of viruses or intrusions, periodic reports, incident recording, and so forth.
- **Availability.** Modern ebusinesses must prevent interruptions of service, even during major attacks. This means that the solution must have built-in fault tolerance and applications and procedures to quickly bring systems back online. IT managers must also be able to make changes to the system 24 x 7.

Privacy for eBusiness

The whole issue of security in an ebusiness environment has evolved to encompass issues of privacy and trust. eBusiness depends on trust between two parties.

The old view of security involved keeping the “bad guys” out by using firewalls, virus protection, and intrusion detection software. The new view adds the model of trusted ebusiness: letting the “good guys” in. These good guys are customers, partners, remote employees, or others upon whom your ebusiness depends. Giving them access is the very basis of ebusiness, but it also adds levels of complexity far beyond the traditional model of security. Security does not require privacy, but privacy requires security. Keeping information confidential requires much more than a technology solution. It is about business policy and the processes they support.

Data privacy is about choice: the freedom of individuals to choose how they wish to be treated by organizations that control data that describes them. For decades, companies have been collecting customer data on computers that have been hidden from public scrutiny. During the past five years, the Internet has brought data collection practices into people’s living rooms. Data privacy has emerged as a major societal issue as individuals have begun to question the levels of technological intrusiveness they will tolerate.

Customer trust depends upon keeping personal information private and secure. Consumers are very concerned about privacy rights and data protection. Government response to privacy concerns has been to create laws and regulations to govern data practices. However, these laws provide minimal protection; business can do more.

Privacy includes several aspects. First and foremost, privacy enables companies to protect personal and organizational assets, such as information about customers and partners; these “good guys” must be let in to access and modify this data, without unauthorized users being able to see it.

Privacy must be built directly into the security infrastructure. Privacy is a matter of policy: determining who can see what within the corporate IT environment. But any privacy policy is only as good as the security infrastructure that backs it up. The security infrastructure doesn’t just improve ROI or the speed at which the enterprise can implement new software, it is vital to the ongoing relationship with partners and customers. As we have seen time and again, customers and partners are not very sympathetic to enterprises that compromise the privacy of their information.

The combination of security infrastructure and a sound privacy policy creates an environment of trust among partners and other users. This protects not only users but the enterprises that hold that data — and which could be held liable for its loss. Access control over proprietary, business-critical data needs to be tighter than that over other types of information, such as publicly available data. Businesses can harness their customers' desire for privacy controls into a strategic competitive advantage.

Implementing Security and Privacy Solutions

There are several steps in installing an ebusiness security solution: creating a blueprint of security needs, selecting skills and resources, and deploying solutions.

The first step in the process is creating a blueprint by assessing security needs and determining how to address them. By definition, these needs should align with the company's business objectives.

There are several stages in creating this blueprint. The assessment stage establishes a baseline or initial diagnosis of the overall security posture. Within the assessment stage are two main pillars: the technical and the business components.

Technical assessments generally involve two main aspects: a vulnerability assessment to determine system weaknesses and a threat assessment to determine likely threats. This stage can also include penetration assessment, or "ethical hacking," which is designed to gain access to the network to pinpoint weaknesses.

The business assessment can contain the following aspects:

- Physical environment assessment covers actual office and hardware.
- Incident response assessment reviews the processes necessary to restore functionality in the event of attack or other incident.
- Information protection assessment examines all policies, procedures, and controls with respect to information access and retention.
- A privacy health check will evaluate all the current processes and procedures, as well as levels of adherence. This check will also evaluate risk of disclosure of personal and confidential data.
- Security awareness assessment of employees.

The next step in the blueprint process is an architectural analysis, which is designed to look at the security solutions already in place and determine what aspects must change. Then

the company must create a security strategy plan to implement these changes.

Selection Process for Skills and Resources

Once the security and privacy needs have been outlined, a company needs to look at its internal resources to determine if it has the necessary skills in-house to implement the blueprint. Some companies will have all the necessary skills in-house, while others must outsource some or all of the implementation. An increasing number of vendors from a variety of backgrounds — consulting firms, security hardware/software vendors, resellers, network integrators, and carriers — are entering and already competing in the security services arena. When looking at resources, companies must answer the following types of questions:

- Does your company have the necessary experience (backed by customer examples and reference accounts) to overcome the security challenges associated with a particular vertical industry or individual business?
- What is the impact of the release of personal information about your customers?
- Have the necessary capital investments been made in tools, staffing, global infrastructure, and support?
- Does your company have alliances with other key industry players to deliver an integrated security service, or is it operating in a vacuum? Are these just “paper alliances,” or are they well coordinated and market tested? If outsourcing with multiple vendors, which vendor would act as the “prime,” and would one have contact with the other solutions vendors?

Once these questions have been answered, the enterprise enters the implementation stage. This phase is key because the company will need to address questions dealing with multiple areas of expertise, encompassing all tasks required to bring the security system to start-up.

On the technical side, as the site is prepared for the integration of the security solution, the hardware and software for the integration must be procured. A combination of the assessment, architecture analysis, and strategy and planning stages will determine whether or not the hardware and software requirements are fulfilled. The company must also decide whether to use a phase-over or cut-over strategy for moving to the new security solution.

Consequently, integration best practices involve the creation of a pilot implementation, which can be performance tested and debugged before migration to the new solution. This practice is

designed to limit downtime, complications, or disruption in business service. Testing and debug services will also continue to play a key role in the implementation of information security engagements because the testing data from such services is used to calculate network device management thresholds and performance baselines.

There are also several human factors to be considered, such as training, staffing, and processes. A perfectly executed integration of the security system is rendered helpless if the IT staff has no idea how to operate, manage, and maintain the network.

Precisely documented policies, procedures, and specifications, in addition to education and training of IT personnel, are critical success factors. In some cases, knowledge transfer may not be necessary or may be subsequently determined during the strategy and planning phase, when a third party is granted the responsibility of managing and monitoring the network — especially if the third party is the one performing the consulting and implementation services.

Selecting and Deploying Security and Privacy Solutions

Enterprises recognize the need to implement security and privacy solutions that can span the end-to-end ebusiness environment. These systems must provide a range of security controls, including intrusion detection, authentication and authorization tools, vulnerability scanning, incident management, and firewall administration. The system must take into account data control processes for sensitive information.

This infrastructure must support a comprehensive common security and privacy model that can expand to new applications and resources. This enables customers to lower their total cost of ownership (TCO), focus on their core competencies, and rest assured their networks are maintained with the latest technologies applicable to their particular needs and vertical industry.

If a company uses an external security service, then it must ensure that the provider is able to not only implement security solutions but, in many cases, manage them on an ongoing basis. For example, intrusion detection services are typically delivered remotely from one or more centralized network operations centers (NOCs) and offer alarm generation and notification, escalation procedures in the case of an intrusion, monthly reporting, and policy recommendations. Other ongoing managed services can include virtual private networks (VPNs), antivirus solutions, Web filtering and content blocking, and routers.

The service will also have to take into account privacy issues for empowering customers to control their own information. Examples of privacy issues include opt-in or opt-out controls for information gathering, data handling procedures, and data retention standards.

Conclusion

As security and privacy threats grow in both scope and sophistication, forward-thinking organizations of all shapes and sizes will continue to strengthen their defenses against these threats. The growing importance of privacy in trusted ebusiness will force enterprises to change the way they approach security. The demands of allowing partners, customers, and sometimes even competitors inside the ebusiness infrastructure will multiply security challenges.

Some organizations will continue to rely on internal systems and resources to manage the cyber risks associated with operating in the new economy. Others, however, may lack the training, skills, resources, or interest needed to operate their IT infrastructure securely and will subsequently turn to outside experts for help.

Over time, the pressure to outsource security and other IT functions will increase. IDC predicts a continued shortage of IT professionals. In fact, due to this highly specialized skill set related to enterprise security, IDC expects the demand for such services from outside firms to eclipse \$17.2 billion by the end of 2004.

But whether a company looks outside or in-house to implement a new security infrastructure, it must take a series of specific steps. Without following this blueprint, a company cannot hope to create a system that is both secure and up to date, encompassing the divergent needs of greater information sharing and greater privacy.

This document was adapted from research published as part of an information service also available by subscription from IDC, providing written research, analyst-on-call, e-flashes, telebriefings and conferences. Visit www.IDC.com to learn more about IDC's subscription and consulting services. Please contact Cheryl Toffel at ctoffel@idc.com, 508-935-4389 for additional copies or Web rights for this document or for related documents.

Quoting IDC Information and Data: Internal Documents and Presentations — Quoting individual sentences and paragraphs for use in your company's internal communications does not require permission from IDC. The use of large portions or the reproduction of any IDC document in its entirety does require prior written approval and may involve some financial consideration. External Publication — 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 2001 IDC. Reproduction is forbidden unless authorized.

www.idc.com.