Managing E-Business Security Challenges

An Oracle White Paper
January 2002

ORACLE

EXECUTIVE OVERVIEW

The new millennium brought with it new possibilities in terms of information access and availability, simultaneously introducing new challenges in protecting sensitive information from some eyes while making it available to others. The Internet allows businesses to use information more effectively, by allowing customers, suppliers, employees, and partners to get access to the business information they need, when they need it. These Internet-enabled services all translate to reduced cost: there is less overhead, greater economies of scale, and increased efficiency. E-business' greatest promise is more timely, more valuable information accessible to more people, at reduced cost of information access.

With the changes in business operations as a result of the Internet era, security concerns move from computer labs to the front page of newspapers. The promise of e-business is offset by the security challenges associated with the disintermediation of data access. One security challenge results from "cutting out the middleman," that too often cuts out the information security the middleman provides. Another is the expansion of the user community from a small group of known, vetted users accessing data from the intranet, to thousands of users accessing data from the Internet. Application service providers (ASP) and exchanges offer especially stringent — and sometimes contradictory — requirements of per user and per customer security, while allowing secure data sharing among communities of interest.

E-business depends on providing customers, partners, and employees with access to information, in a way that is controlled and secure. Technology must provide security to meet the challenges encountered by e-businesses. Virtually all software and hardware vendors claim to build secure products, but what assurance does an e-business have of a product's security? E-businesses want a clear answer to the conflicting security claims they hear from vendors. How can you be confident about the security built into a product? Independent security evaluations against internationally-established security criteria provide assurance of vendors' security claims.

THE NEEDS OF E-BUSINESS SECURITY

While putting business systems on the Internet offers potentially unlimited opportunities for increasing efficiency and reducing cost, it also offers potentially

unlimited risk. The Internet provides much greater access to data, and to more valuable data, not only to legitimate users, but also to hackers, disgruntled employees, criminals, and corporate spies.

Increased Data Access

One of the chief e-business benefits of the Internet is "disintermediation." The intermediate information processing steps that employees typically perform in "brick and mortar" businesses, such as typing in an order received over the phone or by mail, are removed from the e-business process. Users who are not employees and are thus outside the traditional corporate boundary, including customers, suppliers, and partners, can have direct and immediate online access to business information which pertains to them.

In a traditional office environment, any access to sensitive business information is through employees. Although employees are not always reliable, at least they are known, their access to sensitive data is limited by their job function, and access is enforced by physical and procedural controls. Employees who pass sensitive information outside the company contrary to policy may be subject to disciplinary action; the threat of punishment thus helps prevent unauthorized access.

Making business information accessible via the Internet vastly increases the number of users who may be able to access that information. When business is moved to the Internet, the environment is drastically changed. Companies may know little or nothing about the users (including, in many cases, employees) who are accessing their systems. Even if they know who their users are, it may be very difficult for companies to deter users from accessing information contrary to company policy. It is therefore important that companies manage access to sensitive information, and prevent unauthorized access to that information before it occurs.

Much More Valuable Data

E-Business relies not only on making business information accessible outside the traditional company, it also depends on making the best, most up-to-date information available to users when they need it. For example, companies can streamline their operations and reduce overhead by allowing suppliers to have direct access to consolidated order information. This allows companies to reduce inventory by obtaining exactly what they need from suppliers when they need it.

Streamlining information flow through the business system allows users to obtain better information from the system. Now, businesses that allow other businesses and consumers to submit and receive information directly through the Internet can expect to get more timely, accurate, and valuable information, at less expense than if traditional data channels were used.

Formerly, when information was entered into a business system, it was often compartmentalized. Information maintained by each internal department, such as sales, manufacturing, distribution, and finance, was kept separate, and was often

processed by physically separate and incompatible databases and applications — so-called "islands of information." Companies have found that linking islands of information and consolidating them where possible, allows users to obtain better information, and to get more benefit from that information, which thus makes the information more valuable.

Improving the value of data available to legitimate users generally improves its value to intruders as well, increasing the potential rewards to be gained from unauthorized access to that data, and the potential damage that can be done to the business if the data were corrupted. In other words, the more effective an e-business system is, the greater the need to protect it against unauthorized access.

Scalability with Large User Communities

The sheer size of the user communities which can access business systems via the Internet not only increases the risk to those systems, it also constrains the solutions which can be deployed to address that risk. The Internet creates challenges in terms of scalability of security mechanisms, management of those mechanisms, and the need to make them standard and interoperable.

Security mechanisms for Internet-enabled systems must support much larger communities of users than systems that are not Internet-enabled. Whereas the largest traditional enterprise systems typically supported thousands of users, many Internet-enabled systems have millions of users.

Manageability

Traditional mechanisms for identifying users and managing their access, such as granting each user an account and password on each system he accesses, may not be practical in an Internet environment. It rapidly becomes too difficult and expensive for system administrators to manage separate accounts for each user on every system.

Interoperability

Unlike traditional enterprise systems, where a company owns and controls all components of the system, Internet-enabled e-business systems must exchange data with systems owned and controlled by others: customers, suppliers, partners, etc. Security mechanisms deployed in e-business systems must therefore be standards based, flexible, and interoperable, to ensure that they work with others' systems. They must support browsers, and work in multi-tier architectures with one or more middle tiers such as web servers and application servers.

Hosted Systems and Exchanges

The principal security challenge of hosting is keeping data from different hosted user communities separate. The simplest way of doing this is to create physically separate systems for each hosted community. The disadvantage of this approach is that it requires a separate computer, with separately installed, managed, and

configured software, for each hosted user community, providing little economies of scale to a hosting company. Mechanisms that allow multiple different user communities to share a single hardware and software instance, keep data for different user communities separate, and allow a single administrative interface for the hosting provider, can greatly reduce costs for the hosting service provider.

Exchanges have requirements for both data separation and data sharing. For example, an exchange may ensure that a supplier's bid remains unviewable by other suppliers, yet allow all bids to be evaluated by the entity requesting the bid. Furthermore, exchanges may also support "communities of interest" in which groups of organizations can share data selectively, or work together to provide a joint bid, for example.

Assurance

E-businesses need some form of assurance of the security provided in the technology products they purchase. For such assurance, there are international standards used to validate vendors' security claims against established criteria in formal evaluations.

Security evaluations are carried out by independent, licensed and accredited organizations. The evaluation process, from inception to certificate, often lasts up to a full year (and sometimes longer). Vendors who have undergone evaluations of their products learn to improve upon their development, testing and shipping processes as a result of completing the demanding process.

Security evaluations are perhaps the most effective way to qualify a vendor's assertions about its security implementations. Is a product that has not completed such evaluations secure enough to run an e-business? Is it secure enough to protect an organization's most sensitive data? E-businesses demand that the software and hardware vendors they select ship certified, provably-secure products. Assurance afforded by independent security evaluations lets e-businesses be assured of the products they purchase and deploy.

SUMMARY

E-business depends on providing customers, partners, and employees with access to information, in a way that is controlled and secure. Managing e-business security is a multifaceted challenge and requires the coordination of business policy and practice with appropriate technology. In addition to deploying standards bases, flexible and interoperable systems, the technology must provide assurance of the security provided in the products.

As technology matures and secure e-business systems are deployed, companies will be better positioned to manage the risks associated with disintermediation of data access. Through this process businesses will enhance their competitive edge while also working to protect critical business infrastructures from malefactors like hackers, disgruntled employees, criminals and corporate spies.

Managing E-Business Security Challenges
January 2002
Author: Peter Lord
Contributing Authors: Mary Ann Davidson and Kristy Browder

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Oracle Corporation provides the software
that powers the internet.

Oracle is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation. All other product and service names mentioned may be trademarks of their respective owners.

Copyright © 2000 Oracle Corporation
All rights reserved.