

Security, Privacy and Risk Management: 2002 and Beyond

Vic Wheatman, William J. Malik

We forecast likely (and not-so-likely) transformations in the information security marketplace in 2002 and beyond.

ANALYSIS

Current information security, privacy and risk management problems require new or improved solutions, which can provide new domains for theoretical research or commercial exploitation. In 2002, emerging information security technologies have the potential to resolve these issues; as always, however, the eventual resolution will be more nuanced, subtle and complex than what the press releases often propose. We forecast the likely value of several information security tools, products and services in 2002:

- Advanced provisioning will develop as authorization, authentication, privilege and identity management tools overlap in 2002 through 2004, and will converge in products and customized solutions for large enterprises in 2004 through 2006 (0.7 probability).
- Biometric authentication will remain in the advanced technology evaluation stage through 2002; privacy concerns will delay full-scale public- and private-sector implementation of face recognition technology, although niche and high-risk application use will increase. Fingerprint-based authentication will be largely limited to special cases, with fewer than 5 percent of new personal computer procurements requiring integrated biometric readers through 2004 (0.8 probability).
- Web content will increasingly be protected through content validation tools, digital signatures and digital rights management in the face of frequent, high-profile Web content compromises that will erode confidence and threaten intellectual property. Eighty percent of commercial Web sites, and 60 percent of government and nonprofit Web sites, will use one or more of these tools by 2003 (0.8 probability).
- Malicious-code detection and handling tools will change from predominantly signature-based solutions to predominantly behavioral-based solutions by 2005, partly due to the growth of Web services and increasingly active "malware" (0.8 probability).
- Managed-security services will grow in importance, particularly for small to midsize businesses, as the skills needed to manage security continue to be in short supply. However, market consolidation will occur in 2003 through 2004, with larger vendors swallowing the first, innovative providers, which will bring credibility to the market (0.9 probability).

Enterprises currently are examining their information security capabilities in light of a heightened sense of risk. Recent world events illuminate a number of issues that, quite simply, didn't get sufficient attention during normal, day-to-day business activities in 2001. Therefore, in 2002, we will see an increased emphasis on:

- Business continuity to get you back on your feet or avoid the consequences of an outage.
- User authentication to ensure only the right entities use your systems.
- Corporate provisioning to ensure that actual permissions and access rights accurately represent an employer's intention regarding its employees or associates.
- Devices for securing small-office/home-office computing, easing the risk of malicious attack on these systems. Vendors that offer low-cost, highly efficient solutions will enjoy the highest increases in revenue and market share.

- Information openness, such as defining policies governing what information should and should not be publicly available on the corporate Web site.
- Data integrity to ensure that the information available to the public and employees is correct, current and complete.

Enterprises should determine if their organizational structures or business processes are robust and flexible enough to react effectively to crises. We don't expect there will be significant personnel changes resulting from this review, for few enterprises will conclude that an individual's skill set puts the enterprise at risk. Also, many employees often transcend their roles and organizational expectations to solve the problems they face. The lesson for management? People can surprise you if you let them.

Although enterprises currently examine the flexibility and responsiveness of their business processes and organizational structures, very few have yet to integrate physical and information security. Physical security management must have access to correct, current and complete information concerning an enterprise's personnel and physical resources. For most enterprises, this is a directory, provisioning and access issue, not an organizational problem.

In general, security, privacy and business continuity implementations in 2002 will receive the funding and resources they need, even as other areas of the enterprise shrink. For example, many enterprises are finding significant value and leverage with their investments in awareness and training programs. Employees must know the difference between appropriate and inappropriate use of computing resources. This has always been important and is now getting policy-level emphasis. In addition, knowing what to do if there is a security problem has always been important, but until recently, it was assumed that employees and management would have time during a crisis to read their e-mail, attend emergency meetings and figure out what to do. Sept. 11 has taught us that a crisis is the worst time to begin disaster recovery planning.

Features

"The Information Security Hype Cycle" (DF-14-8426). Situating technologies on the hype cycle and forecasting their future progress. **By Victor Wheatman and John Pescatore**

"Remote-Access Authentication: Tokens Rule in 2002" (T-14-9809). How to prove to a computer that you are who you say you are. **By John Girard**

"Security Software Spending in 2001 and 2002" (SOFT-WW-DP-0055). A review of purchasing trends in 2001 and predictions on spending in 2002. **By Colleen Graham**

"Software Security Market Scenarios for 2006" (COM-15-0774). Four market scenarios and factors that will affect vendor market success and enterprise security investment. **By Alain Dang Van Mien**

"Risk Management 2002 and Beyond: Formal and Integrated" (SPA-15-1030). Risk management strategies for enterprises to implement now. **By Simon Mingay**

This research is part of a set of related research pieces. See "Gartner Predicts 2002: Security and Privacy" for an overview.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509