



InSide Gartner This Week Vol. XVII, No. 22, 30 May 2001



## In This Issue...

### Management Update: The Latest Trends in Application Outsourcing

Many CIOs and other enterprise executives are interested in knowing about the latest trends, issues and events in the IT outsourcing market. To help those executives with their planning, Gartner discusses the latest trends in application outsourcing. Quality, shared solution centers, global sourcing and new delivery models are the dominant themes.

#### Gartner's Application Outsourcing Magic Quadrant

The application outsourcing market continues to grow steadily while the nascent offshore market is booming. Despite steady growth, however, the face and composition of the application outsourcing market have not materially shifted during the past few  
*(continued on page 2)*

### Management Alert: Privacy Laws Abroad — Multinationals Must Get Ready or Face Big Problems

Many CEOs and other enterprise executives are extremely interested in insights on what impact the existing and emerging legal frameworks will have on their enterprises' information security strategies. Gartner advises executives of U.S. enterprises with European operations that they must start taking serious steps to comply with European Union (EU) data privacy laws by the end of 2001.

#### EU Data Protection Directive Raises a Storm

Since the EU Data Protection Directive came into effect in 1998, pundits in the United States have made dire predictions about its impact:

*(continued on page 6)*

1

#### Management Update: The Latest Trends in Application Outsourcing

Gartner presents the Application Outsourcing Magic Quadrant. Quality, shared solution centers, global sourcing and new delivery models are the dominant themes.

1

#### Management Alert: Privacy Laws Abroad — Multinationals Must Get Ready or Face Big Problems

Gartner advises executives of U.S. enterprises with European operations that they must start taking serious steps to comply with European Union data privacy laws by the end of 2001.

11

#### Management Update: Cybercrime and the Era of Mass Victimization

The increasing reach of worldwide computer communications networks has changed the economics of crime, and individuals are at risk.

14

#### Management Update: Web Services — Not the Next 'Holy Grail' But Still Great Promise

Web services will drive the next software evolution, succeeding in areas in which earlier technologies have failed.

15

At Random

# Management Update: The Latest Trends in Application Outsourcing (continued from page 1)

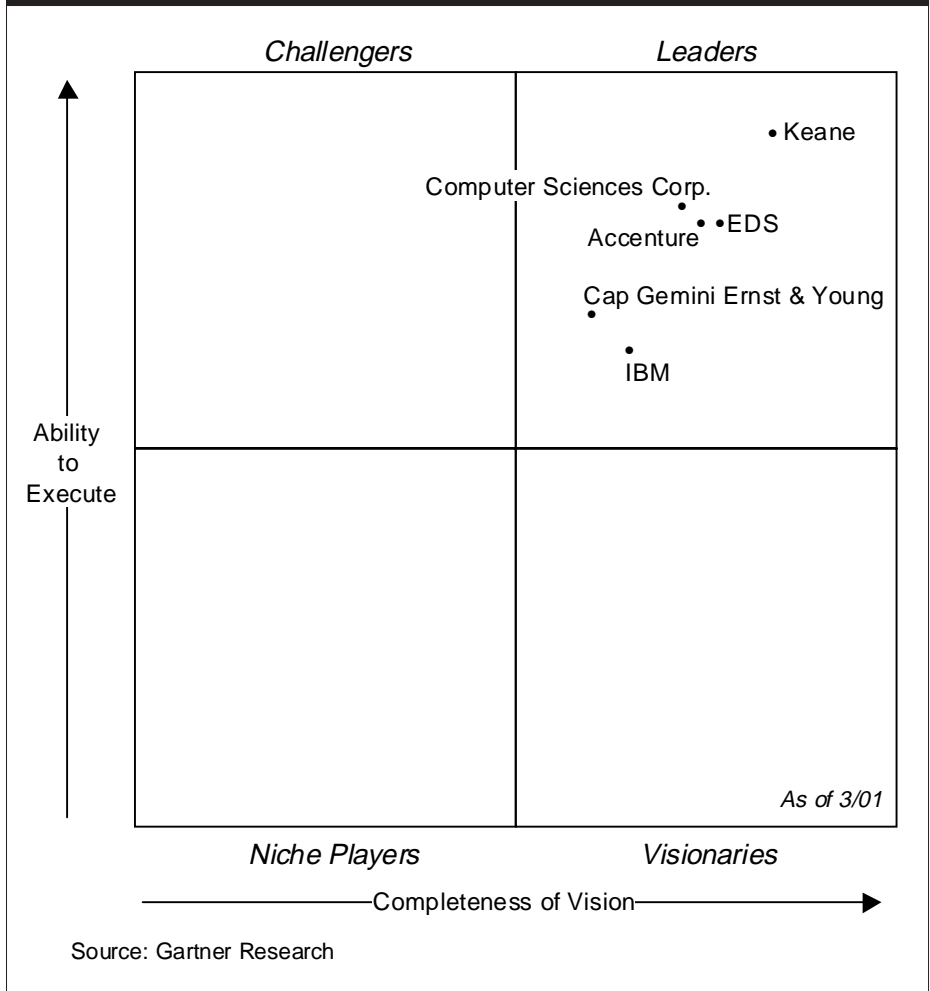
years. Nevertheless, a gradual change in market emphasis was observed during the evaluation process for the latest Gartner Application Outsourcing Magic Quadrant (see Figure 1), which included many interviews with application outsourcing vendors and their customers.

Strong demand has resulted in steady growth in the application outsourcing services market. Gartner believes this growth — driven by the need for skilled IT application labor — will continue. To assist prospective buyers of application outsourcing services, Gartner created the Application Outsourcing Magic Quadrant, which is designed to evaluate vendors based on their completeness of vision and ability to execute that vision.

The Application Outsourcing Magic Quadrant positions six of the largest application outsourcing providers based on their application service offerings and delivery capabilities. Those six vendors are:

- Accenture (formerly Andersen Consulting)
- Cap Gemini Ernst & Young (CGE&Y)
- Computer Sciences Corp. (CSC)
- Electronic Data Systems (EDS)
- IBM
- Keane

**Figure 1**  
**Application Outsourcing Magic Quadrant**



At a minimum, the application services include application management, but they often extend to new development, conversions, migrations and Internet development. Although several of the six vendors also offer IT infrastructure outsourcing services, all will sign stand-alone application outsourcing deals. The

Magic Quadrant evaluation process examined only the vendors' application outsourcing offerings.

### Vendor Positioning

Although all six external services providers (ESPs) ended up in the Leaders segment, differences

Entire contents © 2001 by Gartner, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. Additional subscriptions may be ordered for an annual fee (\$500 in the United States for 50 issues per year; higher pricing may apply elsewhere). Multiple reprint prices are available on request; contact Gartner at +1-203-316-1111. Comments can be E-mailed to: inside@gartner.com.

emerged as seen by the ESPs' respective Magic Quadrant placement.

- Keane, which received the most-favorable client references and feedback, has a heritage deeply rooted in application management and views application outsourcing as its core business and competency. (On average, Keane's deals are somewhat smaller than those of their competitors — although deal sizes are growing — which may tend to favorably skew customer feedback, because there are typically fewer business and IT interface requirements in smaller deals).
- Similarly, although Accenture has many core offerings, the company has always emphasized its application methodologies and processes, something absolutely essential to application outsourcing success.
- CSC, EDS and IBM are all experienced IT outsourcing vendors (i.e., the top three global IT outsourcing vendors in terms of revenue), but the IBM customers interviewed felt that IBM's methodologies did not enable its deals as much as expected.
- CGE&Y is still digesting the merger of Cap Gemini and Ernst & Young and needs some time to capitalize on the strengths of each partner. Furthermore, CGE&Y is the newest entrant to the U.S. application outsourcing market of the six suppliers.

### **Offshore Competition**

The application outsourcing market in the United States traditionally has been dominated by large ESPs as well as a slew of regional and local companies. Recently, a strong offshore programming market has emerged, spurred by increased acceptance of offshore outsourcing. Although Indian vendors dominate today's offshore market with an estimated 80 percent to 90 percent of offshore revenue, other countries have begun to build their own capabilities (e.g., Republic of Ireland, Northern Ireland and Israel). Many companies in other countries (e.g., Russia, Hungary, Egypt, Singapore and Pakistan) are planning to compete for western business. Even China seems poised to participate as enterprise prospects and vendors view the vast potential of its resource pool.

### **Quality Initiatives**

The worldwide Y2K effort raised everybody's consciousness regarding the importance of quality in software development. Similarly, Indian offshore vendors have wholeheartedly embraced the notion of quality (partially to obtain credibility with U.S. enterprises). Many have already achieved Capability Maturity Model (CMM) Level 4 or Level 5 certification for certain projects or development facilities or are in the process of doing so (see the

## **Capability Maturity Model Certification**

The Capability Maturity Model (CMM) was developed by the Software Engineering Institute at Carnegie Mellon University. The CMM is a way to assess the maturity (i.e., strength) of the processes used by an enterprise to develop and support its information systems. Because those processes are the tools by which an enterprise accomplishes its work, the higher its quality, the higher its performance.

sidebar, "Capability Maturity Model Certification"). Others have been focusing on Six Sigma quality efforts, as well as International Organization for Standardization 900x certification.

That has forced U.S.-based out-sourcers to start emphasizing quality initiatives as well, which to date have primarily centered on CMM initiatives. Keane has been in the forefront of CMM efforts, with 32 customer projects independently assessed by assessors authorized by the Software Engineering Institute (SEI) at Level 3 and two at Level 4.

Because the average U.S. IS organization would find itself rated at CMM Level 1 or Level 2 (see the sidebar, "CMM Assessment Levels in SEI Data Pool"), outsourcing can provide an effective means of accelerating the adoption of CMM-based practices (see the sidebar, "CMM Initiatives

## Management Update: The Latest Trends in Application Outsourcing (continued)

### CMM Assessment Levels in SEI Data Pool

CMM Level	Percentage of Assessments
Level 1	32.2
Level 2	39.3
Level 3	19.4
Level 4	5.4
Level 5	3.7

Source: SEI from data spanning 1996 through December 2000. Taken from 1,798 assessments, 4,783 projects and 1,012 organizations (32.7 percent offshore)

### CMM Initiatives in the United States

In the SEI's study, a trend was noticed toward higher maturity profiles for offshore organizations compared with U.S. ones. In general, most U.S. enterprises are aiming at Level 3 certification for their customers, because most U.S. customers question whether the return on investment of levels above that justify the investment, except where the project or business demands these levels (e.g., certain defense initiatives). In U.S. enterprises, services and manufacturing industries are conducting the most software assessment processes.

in the United States"). That can help enterprises compete more effectively in today's competitive business environment, because each higher CMM level brings a series of tangible improvements in

the cost, efficiency, time-to-market and quality of an enterprise's deliverables.

However, despite the stated interest of vendors and enterprises in these initiatives, most ongoing application outsourcing deals that Gartner reviewed during the Magic Quadrant process were not focused on quality endeavors. That was true even though most of the ESPs participating in the Magic Quadrant process emphasized their CMM certification levels and efforts.

#### Effective Resourcing

Outsourcers are increasingly focusing on effective resourcing (i.e., ensuring that the right skills are delivered at the right time for the right price). Surprisingly, most outsourcers in the past did not have effective, automated global systems that told them exactly where in the world a particular skill set could be found and whether it would be available in the required time frame. ESPs are now developing or have implemented global resourcing systems that enable them to instantly access such information.

#### Shared-Solution Centers

Other resourcing strategies involve creating virtual teams and implementing shared-solution centers that focus on a specific vertical, technical competence or geography. That results in a lot of work being shared offsite by staff members who are the most experienced in the required

disciplines (e.g., EDS has more than 100 such solution centers around the globe). Those shared-solution centers usually result in more cost-effective, high-quality resources and can be viewed as the economy of scale backbone for application management and development efforts.

#### Global Sourcing

Spurred by an increasingly competitive market, with many new, lower-cost providers competing for the work, U.S. vendors are implementing global delivery models through geographically dispersed, offshore delivery centers with the goal of doing work where it makes economic sense and in providing, in some cases, 24x7 service.

Most are also investigating alternative global delivery models, including partnering with established offshore companies to do certain development and maintenance activities (e.g., CSC and Cognizant Technology Solutions), establishing joint ventures overseas (e.g., Perot Systems and HCL formed HCL Perot Systems) and establishing wholly owned subsidiaries overseas.

Many are building, or have already established, solution centers offshore or nearshore. CGE&Y has announced a 250-person facility in Mumbai, India, which is part of its worldwide network of 40 solution centers called Accelerated Delivery Centers. PricewaterhouseCoopers opened its Center of Excellence for Oracle-based customer relationship

management suites in its Technology Center in Calcutta. Many other examples of offshore solution centers exist, such as:

- Accenture: The Philippines
- EDS: Global competitive solution centers in Australia, Brazil, Canada, Egypt, India, Mexico and New Zealand
- Keane: Canada

### **Global Consolidation**

Large, global ESPs are also trying to establish capability overseas to better support the local offices of their global clients. Those efforts are primarily focused in Europe and Asia/Pacific, with some small efforts in Latin America. Gartner believes this, along with increasing interest in outsourcing overseas, will foster a new wave of mergers and acquisitions in the application outsourcing market, as the large global players acquire smaller local firms that have a knowledge of local customers, culture and business practices, but lack the depth and breadth of the larger service providers. Additionally, many Indian vendors are evaluating the acquisitions of various consulting firms in the United States and Europe as a way to increase their competitiveness in those countries and offer higher-value consulting services.

### **New Delivery Models and Partnerships**

Many application outsourcing suppliers are experimenting with

newer, emerging forms of application outsourcing delivery models, such as application service providers (ASPs), hosting, applications infrastructure or various Web services.

- EDS has announced a broad set of ASP services (EDS Application Hosting).
- IBM's Prime offering provides various Web and applications hosting services for independent software vendors and ASPs.
- Accenture has invested in Jamcracker, an ASP aggregator.
- CGE&Y has an investment in Corio, a leading enterprise ASP.
- Deloitte Consulting recently announced an investment in ASP Intira.

Interestingly, the established outsourcing vendors — which Gartner believes have the potential to be the most successful ASPs — are reluctant to actively push this model, because the underlying economics are quite different from their business models.

### **Greater Customer Satisfaction**

Despite many complaints about their deals and vendors, enterprises seem to be more satisfied with their application outsourcing deals than in past years. Gartner believes this is because of increased vendor experience and flexibility and greater user

sophistication. Increased satisfaction levels were also noted during Gartner's IT outsourcing Magic Quadrant assessment where the five vendors evaluated were all positioned in the Leaders segment.

### **Bottom Line**

- Application outsourcing exhibits solid growth and enterprises are more satisfied than in the past.
- Competition is increasing, particularly from offshore vendors with lower rates and, in some cases, equal or better quality.
- The market is slowly evolving toward a complete global resourcing model where skills are delivered where and when they make sense.
- Shared-solution centers, global sourcing and new delivery models will be the model for the future IT supply chain.

Written by Edward Younker,  
Research Products  
Analytical source: Rita Terdiman,  
External Services Providers

*For related articles in Inside Gartner This Week, see:*

- "Management Update: Be Aware of the Approaching ASP Market Consolidation," 21 March 2001
- "Management Update: The Importance of Understanding ASP Offerings," 14 March 2001
- "Management Update: The Importance of Understanding the ASP Hype Cycle," 7 March 2001
- "Management Update: The Evolving ASP Marketplace," 28 February 2001

---

## Management Alert: Privacy Laws Abroad — Multinationals Must Get Ready or Face Big Problems (continued from page 1)

- Some have predicted that international information trade wars will break out as a result of the new laws.
- Others have suggested that the compliance costs for U.S. businesses will be astronomical.
- Many have compared the consequences of the legislation with the year 2000 “crisis.”
- The directive has also been labeled as being bureaucratic, an intrusion on American sovereignty — “Eurocrats” in Brussels telling U.S. companies what to do — and unenforceable.

### Not Quite So Bad

None of those views reflects an accurate understanding of the EU laws. The responsibilities outlined under the directive, and the resulting national laws, are not as onerous as has been widely reported. For example, opt-in (explicit consent) is required only in narrow circumstances in most EU countries.

The greatest challenge for enterprises, and for the authorities enforcing the regulations, will be to determine how the regulatory provisions translate into actual business and IT policies and practices. Indeed, certain companies, particularly U.S. enterprises with operations in Europe, will inevitably need to make significant changes, especially in their treatment of

human resources (HR) and customer data, and in their arrangements with business partners and service providers.

### Addressing Some Key Questions

Most EU-based enterprises already have some experience with dealing with data protection laws, and in any case, there is not the same level of rampant personal data sharing and selling in Europe as in the private sector in the United States. The greatest challenge posed by the directive for enterprises within the EU will be to discover what changes the regulatory provisions will require in their business and IT practices. Among the questions that EU enterprises will have to answer are:

- Is permission required every time a new use is discovered for a customer’s data?
- How all encompassing can a “blanket” up-front disclosure be?
- Will changes to new and installed applications and systems — such as customer relationship management, marketing and HR implementations — be required?
- Would it be better to make all data blind than to go through the burdensome process of meeting notification requirements?

What the directive, and its implementation via national laws, will

mean in practice is still largely undefined by the national data protection authorities in the EU. There are also significant differences in national implementations. Belgium, France, Denmark and Germany, for example, have extended the “sensitive” category, which requires explicit consent by the individual, to include financial information, national identifiers and the building of “profiles.” There are, however, broad exemptions for the processing of certain types of data.

### Compliance Requirements

Despite the uncertainties, some basic aspects of the EU directives are clear. Compliance will require enterprises operating in the EU to:

- Determine how they will use personal information pertaining to customers or employees, and then create and administer the requisite disclosure policies to customers, either online, via call centers or at physical locations.
- Update their information security practices.
- Be prepared to comply within a certain time period with requests from employees or customers to view information that an enterprise is holding about them.
- Notify local data protection authorities concerning how they use data about individuals in certain cases.

## Controversial Aspects

Among the most controversial aspects of the EU legislation is its prohibition on the transfer of EU personal data to countries without privacy legislation that is deemed adequate by the European Commission. Enterprises located in countries with inadequate privacy legislation that use or store

personal data generated in the EU are required to obtain the explicit consent of the individuals involved and gain permission from the national data protection authorities of the relevant countries by guaranteeing that personal data will be adequately protected when it is transferred.

Due to the absence of comprehensive data protection laws for the private sector in the United States, the U.S. Department of Commerce and the European Commission spent several years haggling over a suitable arrangement — the Safe Harbor program, which came into effect in November 2000. The Safe Harbor program would allow U.S.

## The Safe Harbor Agreement Between the European Commission and the U.S. Department of Commerce

**T**he Safe Harbor program allows U.S. businesses with operations in Europe not to have to undergo the significant burden and expense of obtaining permission from national EU data protection authorities, and requires slightly less-stringent privacy protections than the national implementations of the directive.

U.S. enterprises that sign up for Safe Harbor will meet the EU's adequacy requirements, and will be able to process EU personal data in the United States. Those enterprises must ensure that they treat EU personal data according to the main provisions of the directive — those concerning notice, choice, access, security, data integrity and equivalent protection when personal data is transferred to third parties, and enforcement.

EU enterprises must verify their compliance with those provisions and provide for dispute resolution, either by signing up with a private "seal" program or by agreeing to be overseen by a supervisory agency, such as the Federal Trade Commission (FTC) or the Department of Transportation (for airlines), or by an EU data protection authority.

The most burdensome requirements will be providing for choice (opt-in for sensitive information, opt-out for use of information not covered by the initial disclosure) and access to data. The access requirement is much more lenient under Safe Harbor than under the EU Data Protection Directive and national implementations;

access does not have to be granted in certain cases if doing so would be too costly for the business.

The Safe Harbor program faces some challenges:

- Certain industries (e.g., U.S. financial institutions) are not eligible to participate in the program. U.S. financial institutions with European operations must either negotiate separate contracts with EU authorities or obtain adequacy via other routes, such as explicit consent for personal data transfer to the United States from EU employees.
- Private verification and audit programs available in the United States are limited and inadequate. A further retrenchment from the FTC's current involvement in privacy matters could jeopardize the Safe Harbor program and, consequently, the ability of U.S. enterprises to process EU employee or customer data in the United States.

It could be argued that the European Commission agreed to the program only because the FTC agreed to police U.S. businesses that signed up for the program. The regulatory philosophy of Timothy Muris, the recently appointed chairman of the FTC, however, suggests that he is not only likely to continue the self-regulatory approach to privacy protection, but may actually reduce the increased involvement of the FTC in this area.

---

## Management Alert: Privacy Laws Abroad — Multinationals Must Get Ready or Face Big Problems (continued)

enterprises to continue to use EU personal data in the United States (see the sidebar, “The Safe Harbor Agreement Between the European Commission and the U.S. Department of Commerce”).

### U.S. Multinationals Balk

To date, fewer than two dozen companies have signed up for this voluntary “self-certification” program, which requires U.S. enterprises to adhere to the basic principles of the directive and agree to be overseen by the Federal Trade Commission (FTC), other national regulatory authority or an EU national data protection authority. The unimpressive response by U.S. enterprises to Safe Harbor can be explained by three factors:

- Many major U.S. multinationals that regularly process EU employee or customer data in the United States have long-standing relationships with national data protection authorities, and are already working with them on the specific requirements of their national laws, and with other enterprises in their industry sectors on codes of conduct.
- Questions remain about whether Safe Harbor will actually shield enterprises from legal liability for noncompliance with the EU directive in all cases. Some U.S. multinationals believe that their first priority should be to work

with national data protection authorities to deal with the most critical cross-border data flows — usually HR data — and then decide whether it is beneficial to join the Safe Harbor program.

- The overwhelming majority of U.S. enterprises do not appear to consider the EU data protection laws to be a serious, imminent business and legal risk. This, coupled with a general state of unreadiness within enterprises to comply with the provisions of Safe Harbor, accounts for the minimal response to the program.

### July 2002 Deadline

Does this complex and somewhat ambivalent regulatory climate mean that the majority of U.S. enterprises that use EU personal data will face serious problems? Indications are that this is not an imminent danger.

It is worth remembering that the EU does not yet have its own house in order with regard to the directive. Some EU member states, such as France and Germany, have not yet passed laws based on the directive; other countries’ laws have only just taken effect. The national data protection authorities — the main investigators and enforcers of the directive — are focused on determining what will constitute compliance with the new laws and working with industries on codes of conduct for their sectors.

Moreover, the Safe Harbor program provides for a grace period; U.S. enterprises have until July 2002 to sign up, and EU authorities are unlikely to take action against them before the deadline.

### Noncompliance Enforcement Actions

Nonetheless, Gartner believes that by the end of 2001, EU data protection authorities will begin non-compliance enforcement actions against at least a handful of U.S. enterprises with European operations, probably over violations to HR data policies. The actions will range from large fines to protracted lawsuits that prevent the transfer of data.

As U.S. enterprises begin to recognize the burden and expense of understanding and complying with multiple national requirements of the EU countries in which they operate, the number of applications for Safe Harbor certification will increase dramatically. However, by that time, the agreement may be in danger.

### Noncompliance Risks

By 2002, Gartner expects 40 percent of U.S. multinationals to adhere to the higher data protection standards set by the EU through deidentification of personal data and employee consents and contracts with data protection authorities, and the Safe Harbor program (0.7 prob-

ability). The remaining 60 percent of multinationals, along with U.S. enterprises with operations in Europe, will either keep and process EU personal data in the EU or be noncompliant.

Those that remain noncompliant will bear the business and legal risks of potentially being singled out for enforcement. The number of such enforcements will increase significantly through 2002, as relations between the U.S. administration and the EU on the issues of privacy and personal transborder data flows deteriorate.

### **Managing Data Differently**

U.S. enterprises that process EU employee or customer data in the United States will have to collect, store, allow access to and manage that personal data in a manner that is often different from the way U.S. personal data is treated. Those enterprises will have to decide whether to manage that data differently from U.S. data — and, if so, how — or to manage all personal data in keeping with the higher standards required by EU privacy laws.

### **Other International Areas**

The EU Data Protection Directive and its national implementations are not the only international data protection laws that U.S. enterprises with a global presence will face. Canada recently passed the

C6 Act, which is now in force for regulated industries (telecommunications firms, financial institutions and transportation companies), and will apply to certain types of cross-border data transfers. Hong Kong and Argentina also have data protection laws that are similar to the EU directive.

By the end of 2002, Gartner expects 30 percent of U.S. multinationals to have in place global data privacy standards for customers that will allow personal data to be transferred and processed anywhere, irrespective of the origin of the data (0.7 probability).

### **Key Facts**

- The EU Data Protection Directive was passed in 1995, after years of negotiations. The main purpose of the directive is to ensure that a minimum standard of data protection exists so that personal data can be transferred between member states. Before the directive, a significant lack of uniformity existed between data protection laws in the various EU member states (for example, Greece and Italy had none at all).
- Article 26 of the directive prohibits personal data transfers, without the express consent of the data subject, outside the EU to countries where privacy protection laws are deemed to be inadequate. Some EU member states already

had such prohibitions in their national data protection laws; others, like the United Kingdom, did not.

- The directive has five basic provisions:
  - Individuals must be given notice regarding how their personal information will be used, strictly stating the purposes for how the information will be used and storing it only as long as is needed.
  - Individuals must have the ability to see what information is being kept about them.
  - Enterprises must ensure that personal information is properly protected.
  - Enterprises must receive explicit consent (opt-in) from individuals when transferring sensitive categories of information, such as religious, trade-union and health data, to third parties.
  - Individuals have wider rights to complaint about violations of their privacy, and the national data protection authorities have stronger investigatory and enforcement powers.
- Enterprises should be aware that they are required to notify

---

## Management Alert: Privacy Laws Abroad — Multinationals Must Get Ready or Face Big Problems (continued)

national data protection authorities about how they are using personal data. Each EU member state has to implement the provisions via new national legislation or amendments to existing laws. This legislation has, however, only recently been passed, or has only recently come into effect, in most EU member states. For this reason, many of the consequences of the directive remain unclear.

- Some competing standards have been put forward by the EU Data Protection Directive, the EU Telecommunications Data Protection Directive and the proposed Electronic Communications Directive. For example, most of the national data protection laws require opt-out for direct marketing (some member states require opt-in); the Telecommunications Directive requires opt-in, and the EC Directive requires opt-in for e-mail marketing. The distinctions are largely irrelevant, because most e-mail

marketing campaign management tools and services have turned to opt-in, and usually double opt-in.

### Bottom Line

- U.S. enterprises with operations in Europe should take seriously the risks of noncompliance with the EU Data Protection Directive.
- Breathing room will exist for most of 2001, but national data protection authorities are likely to begin actions against companies in the consumer industries over customer and HR data practices by the end of 2001.
- By 2002, Gartner expects 40 percent of U.S. multinationals to adhere to the higher data protection standards set by the EU through deidentification of personal data and employee consents and contracts with data protection authorities, and the Safe Harbor program (0.7 probability). The remaining 60 percent of multinationals, along

with U.S. enterprises with operations in Europe, will either keep and process EU personal data in the EU or be noncompliant.

- By the end of 2002, Gartner expects 30 percent of U.S. multinationals to have established global data privacy standards for customers that will allow personal data to be transferred and processed anywhere, irrespective of the origin of the data (0.7 probability).

Written by Edward Younker,  
Research Products  
Analytical source: Arabella Hallawell,  
Information Security Strategies

*For related articles in Inside Gartner This Week, see:*

- “Management Update: Caught in the Net — Online Monitoring and Employee Privacy,” 18 April 2001
- “Management Update: Data Privacy — It’s Not What You Do, It’s the Way You Do It,” 6 September 2000

---

# Management Update: Cybercrime and the Era of Mass Victimization

**E**nterprise executives, employees and individuals at large are all facing increasing information security risk. Gartner points out that the increasing reach of worldwide computer communications networks has changed the economics of crime, and individuals are at risk.

## **Criminals in Cyberspace**

The nature of malicious code — code whose explicit intention is to victimize the unwitting — has changed significantly since 1998. Increasingly, the purpose of such code is to surreptitiously read or steal a person's personal information. A separate, and reinforcing, technology trend is the widespread use of passwords for electronic authentication and signature. Those two trends in combination provide criminals, who already possess motive, with means and opportunity, and will likely lead to a series of mass identity theft attacks (i.e., attacks in which legitimate identification is used by unauthorized persons to impersonate the real owner for criminal purposes).

## **The Potential for Misuse of Surreptitious Code**

The technologies required to initiate such attacks are simple and widely available, and in some cases have already been deployed for ostensibly

benign purposes by commercial applications.

One example is Netscape's SmartDownload (which, in previous versions, surreptitiously tracked and reported to Netscape on the materials downloaded from Internet sites by the programs' users). SmartDownload monitored inbound and outbound Internet traffic to a user's machine; it would be no more difficult to silently scan a user's hard drive for passwords (which through 2002 will serve the majority of users as default electronic IDs and signatures), account numbers, and other information that could be used to initiate commercial transactions.

Indeed, consumer applications and devices increasingly have the ability to track customers' behavior, usage habits and the information that is given out to Web sites, without the customer knowing such monitoring is occurring. Recent legislation introduced in the U.S. House of Representatives seeks to ban such surreptitious code from use by legitimate businesses; but that will not deter criminals from using these techniques.

In addition, new wallet, buying-agent and aggregation services and other applications that offer consumer convenience are frequently designed to

pass information back to a home server on a routine basis, or store identity information entirely on the wallet or aggregator's servers. Centralized storage of such information en masse is obviously an attractive target for hackers and disgruntled insiders. The significant security investment and expertise required to appropriately protect such information will be a major challenge for many providers of such services.

## **The Danger of Password-Stealing Programs**

Malicious codes frequently contain password-stealing programs as part of their payload. Password-stealing programs — or other programs that steal private keys and other identity information from the end user's machine — are usually in the form of "Trojan horses," a malicious program disguised and triggered by a user due to a benign or luring appearance, such as an e-mail from a friend or a cartoon attachment.

Recent well-known malicious code incidents, such as the PrettyPark virus and the executable part of the "ILOVEYOU" virus, contained password-stealing programs and show that such programs are currently feasible as a means of attack on a mass scale, even in cases where target machines are protected by firewalls.

---

## Management Update: Cybercrime and the Era of Mass Victimization (continued)

These viruses have in general been discovered quickly only because their creators insisted on making them visible (presumably because the individuals involved were thrilled by the notoriety their creations afforded them). There is no reason to believe that all criminals will make their Trojan horses so visible. In the absence of overt signals from such a virus, there is no way, in most cases, for a typical user to discover that the virus is present. In fact, absent such overt signals, it is unlikely that even the vendors of antivirus software would be aware of the malicious code. In other words, even a user who diligently performed regular upgrades on his or her antivirus software might be victimized.

Such virus attacks are, as a rule, eventually discovered, but days, weeks or months might pass before discovery. In the meantime, the perpetrator has ample opportunity to collect and either use or resell valuable information. The fact that any individual victim (compared to a large corporation) may have limited resources available to steal is unimportant to potential criminal profitability. In the age of the networked economy, it is just as profitable (and feasible) to steal small amounts simultaneously from thousands of people as it is to steal a large amount from a single corporation. It may even be more feasible; people are likely to be less well-protected than the corporation.

A second path to mass victimization was demonstrated recently by the PayPal “spoof,” in which a criminal succeeded in redirecting Web traffic aimed at the PayPal site to a mock PayPal site. There is little opportunity for an end user to verify that the site he or she is visiting is in fact the “real” site. In such cases, the criminal activity is likely to be more quickly discovered; this only places a requirement for speed on the criminals — which is nothing more than the cost of doing business in the Internet era.

### **Criminal Work for Idle Hands?**

A factor inhibiting attacks of the type described above is the presence of a strong international market for employment of skilled technologists at good wages. In other words, most of the people who can execute the kinds of attacks described above can find honest work, and do not have to turn to crime to make a living.

Gartner has predicted that through 2003, a gap will exist of at least 20 percent worldwide between demand for skilled technologists and available supply (0.8 probability). However, there are persistent fears in the financial markets concerning the potential for worldwide recession, which may affect employment opportunities for technologists; and many skilled technologists are now in countries such as Nigeria and the former Soviet Union for whom legitimate job opportunities are already limited.

The recent attacks on Microsoft that resulted in the apparent theft of operating system source code apparently originated in the Ukraine, and used a Trojan horse approach to gaining entry. The intrusion was detected, months after the fact, only by the discovery in Microsoft’s system logs of unusual outbound traffic from Microsoft’s Web servers.

Gartner research has stated that law enforcement is inadequate to the task of policing cyberspace, and will likely remain so. Through 2004, annual federal (United States) funding for cybercrime training, investigation and enforcement will likely not exceed 1 percent of the overall federal law enforcement budget (0.7 probability).

Moreover, internationally, attitudes toward law enforcement aimed at cybercrime vary dramatically. There is nothing like a common international legal code for cybercrime, nor is there any organization chartered and authorized by governments worldwide to create such a code. This is significant, because cybercrimes are easily internationalized; the technology and the human talent required to execute them can easily be exported when necessary to evade law enforcement or to take advantage of a lax enforcement environment.

Through 2004, driven by awareness of the inadequacies of cyberlaw enforcement and by increasing

criminal opportunities, the economic value represented by cybercrimes will increase by two to three orders of magnitude, i.e., by 1,000 to 10,000 percent (0.6 probability).

By the end of 2002, at least one incident of mass, surreptitious victimization of thousands of Internet users will have occurred in which the object was not vandalism but theft (0.8 probability). Given the nature of the crime, and the state of international law enforcement on the Web, the identity of the thief will remain unknown (0.7 probability).

### How to Protect Yourself

Given this environment, it is clear that individuals must take steps immediately to protect themselves. Gartner recommends in particular that individuals do the following:

- Install a personal firewall on any (noncorporate-supported) computer that has Internet access, especially on those that contain files that might enable unauthorized access to financial accounts or other critical information.
- Monitor financial transactions carefully and frequently, looking for any evidence of unauthorized or otherwise unexplained transactions such as purchases, fund transfers, or withdrawals. Illicit transactions may be minor (e.g., less than \$10). It is especially important to monitor transactions

following major holidays, such as Christmas, when high transaction volumes can serve as a “smoke screen” for fraud.

- Use a credit card with a low balance limit exclusively for online transactions (and for no other purpose). Debit cards should not be used for online purchases unless the user has confirmed that the issuer assumes liability for fraudulent transactions.
- Read the privacy policies or terms of use agreements of new media, aggregation services or applications before you download them.
- Do not use “online wallets,” one-click buying or account aggregation services that store personal credit and financial information on any Internet-connected server, or anywhere else that is not under the direct control of the information’s owner.
- Disable active content functionality (ActiveX and Java) on any Internet-connected machine.
- Install virus protection software and update it on the vendor’s recommended schedule for online updates.
- Disable Microsoft peer-to-peer networking on any Internet-connected machine.

- Consider subscribing to a scanning or monitoring service from your Internet service provider, cable access or DSL (digital subscriber line) provider.

### Bottom Line

- Multiple converging technology trends that take advantage of network-based economies of scale will soon create a new class of “mass victimization” crimes.
- Law enforcement agencies are poorly positioned to combat these trends. Individuals must act to protect themselves, beginning with awareness that the potential for victimization exists, and that the relative anonymity of an individual compared to a corporation is no protection.

Written by Edward Younker, Research Products  
Analytical sources: Arabella Hallawell, Richard Hunter and Neil MacDonald, Information Security Strategies

For related articles in *Inside Gartner This Week*, see:

- “CIO Alert: Managed Vulnerability Services Will Beat Hackers to the Punch,” 28 March 2001
- At Random, “Zimmermann’s Move Raises Questions About Pretty Good Privacy’s Future,” 21 March 2001
- At Random, “A Lesson in Managing Security Risks of New Technologies,” 28 February 2001
- At Random, “Microsoft’s DNS Woes Highlight Vulnerability,” 21 February 2001

---

# Management Update: Web Services — Not the Next ‘Holy Grail’ But Still Great Promise

**B**ecause it is so important to their businesses, many CIOs and other enterprise executives are keenly interested in insights on how Internet-derived technologies will evolve over the upcoming years. To assist those executives with their planning, Gartner points out that Web services — simple in nature and timely in their emergence — will drive the next software evolution, succeeding in areas in which earlier technologies have failed.

## **Great Promise for Web Services**

Several years ago, component technology and distributed computing promised to transform leading-edge businesses into agile, globally connected enterprises via the reuse of code, the use of idle compute resources, and drag-and-drop “no programming necessary” tools. However, simply put, that didn’t happen.

Today, Web services carry many of the same promises of those technologies of the past; but unlike its predecessors, the industry’s latest tour de force stands a much greater chance to deliver on its promises.

## **Why It Will Happen This Time**

Web services technology derives significantly from component technology. In fact, Gartner’s definition of Web services as “software components accessible over ubiquitous networks” leverages a great deal

from the concept of component technology. However, despite this and other similarities to previous technologies, Web services will fulfill these long-unfulfilled promises to some extent. To understand why this is so, one must first understand what has changed.

First of all, between the last “component revolution” in the mid-1990s and today, the Internet happened. And the Internet has affected almost everything. The potential of Web services is enhanced because Web services use Internet technologies. But that isn’t the main reason why the environment is so ripe for Web services. The cause is more cultural and relates directly to the most difficult barriers that component technologies faced during their heyday. Three areas in which the culture (and to a lesser extent, the technology) has changed are reuse culture, semantic agreement and simplicity itself.

## **Reuse Culture**

The culture of the Internet encourages reuse and sharing. Many Web developers get inspiration and initial code by using HTML and other code from existing Web sites. If asked to include a stock ticker or weather forecasting capability on a Web site, today’s developer would almost certainly opt to leverage the primitive Web services that are available rather than trying to build from scratch. The ability to view and download Web

pages to use as starting points in projects is also a phenomenon that contributes to the reuse culture. Note, however, that not all reuse cultural barriers have been removed. Although the practice is slightly less prevalent today, productivity measured by lines of code and the “Not Invented Here Syndrome” still lives on.

## **Semantic agreement**

It was often said that components would never work because you’d never get agreement on what the data in and out of the component meant. And regardless of how far technology progressed, that potential problem would be insurmountable. Although Web services represent no breakthrough in technology, their ability to use public (or semipublic) registries through standards such as UDDI (Universal Description, Discovery and Integration) makes that point much less valid. A Web service’s interfaces are simply published. If someone wants to use them, the person can. If not, that’s fine, too — because the person can search for another service, map the inputs and outputs differently, or create his or her own service. The agreement is simple. The writer proposes; the consumer agrees by using, or disagrees by not using. A simple idea, powered by a simple concept (the public registry).

---

## Simplicity Itself

Internet standards help here, but again, it is much more of a cultural factor. Web services will not succeed unless they are simple. Because they must be usable by a class of Web developer with less skill (for example, a business unit developer), Web services approaches must be simpler. Amazingly, however, simplicity seems to be the cultural piece with which most vendors and developers remain uncomfortable. Vendors and developers alike are constantly stretching to escape from simplicity. To succeed, they must

view the simplicity of Web services as an asset, not a restriction.

## Bottom Line

- Web services do not represent the “Holy Grail” of computing, but they do get closer to delivering on many of the broken promises of years past.
- Enterprises should have realistic expectations and should be prepared to reap some of the benefits of earlier promises (e.g., reuse), but should not expect the utopian benefits previously promised.

Written by Edward Younker,  
Research Products  
Analytical source: David Smith,  
Internet Strategies

*For related articles in Inside Gartner This Week, see:*

- “CIO Update: Web Services Pioneers — A Vendor Update,” 23 May 2001
- “Management Update: The Future of Web Services — Dynamic Business Webs,” 23 May 2001
- “Management Update: What Is .NET and Why Should Enterprises Care?” 16 May 2001
- “Management Update: Web Services and Software E-Services — What’s in a Name?” 29 November 2000

---

## At Random

**Microsoft Hits Enterprises With Huge Price Jumps on Software Licenses.** On 10 May 2001, Microsoft unveiled its new version 6 licensing programs — Open, Select, Enterprise Agreement and Enterprise Agreement Subscription. Microsoft will replace its version 5 programs on 1 October 2001.

The substantial, complex changes Microsoft has made to its licensing programs will affect all Microsoft software products and customers. The main effects include:

- Enterprises with four-year upgrade cycles for Microsoft Office will typically pay 68 percent to 107 percent more to upgrade.
- Those with three-year upgrade cycles will typically pay 35 percent to 77 percent more, depending on their volume discount level.

Microsoft believes it has simplified its licensing; Gartner believes Microsoft confuses simplification with the elimination of options. Either way, most enterprises will pay much more. A typical enterprise with 5,000 desktops that upgrades Microsoft Office every four years will have its fees increase from \$900,000 to \$1.7 million.

---

## At Random (continued)

The following three parts of the announcement will have the most significant effects:

- **Elimination of Version Upgrades** — Microsoft will eliminate Version Upgrades (VUPs), Product Upgrades, Competitive Upgrades and Language Upgrades. VUPs offer the lowest-cost upgrade mechanism for enterprises upgrading less than twice every two to three years. Most Microsoft customers use them. Customers now have two choices: rebuy the licenses, or buy Software Assurance (SA), formerly called Upgrade Advantage (UA).
- **SA Replaces UA** — SA now becomes the only way to upgrade, apart from rebuying the license. SA is priced annually at 29 percent of the license cost for desktop products and 25 percent for server products. In most cases, these prices are lower than UA prices, but they are not lower than VUP prices and are significantly higher than industry norms of 17 percent to 22 percent.

Furthermore, Microsoft does not include technical support in SA as do most other vendors. SA provides perpetual rights to versions released during the term of the agreement. However, if enterprises want SA, they must buy it at the same time they buy the license. The break-even for SA is about three and a half years. Gartner recommends the following:

- Enterprises that upgrade every three years should buy SA
- Enterprises that upgrade every four years or longer should rebuy the software
- **Subscription Pricing Now an Option Under Enterprise Agreement (EA)** — This new offering of nonperpetual licenses is available for enterprises with 250 or more PCs and is priced at 85 percent of the cost of the perpetual license. Microsoft calculates the break-even point at five to six years.

Given the degree of lock-in with this license agreement, Gartner does not believe the price will attract most enterprises. To ease concerns, though, Microsoft offers a buy-out clause for the end of the third year for one and a half times the third-year fee. However, Gartner believes that by 2005 Microsoft will eliminate buy-out clauses from Subscription Agreements (0.7 probability). Enterprises not exercising the buy-out option must renew their subscription or uninstall the software. Gartner recommends the following:

- Enterprises considering subscription licenses must carefully analyze the total cost over the entire period the application will be installed, including the buy-out clause, and compare this to the perpetual EA or Select licenses.
- If subscription is appropriate, enterprises should negotiate for a price cap of 5 percent to 8 percent for subscription renewals.

Analytical sources: Alexa Bona and Alvin Park, Software Asset Management

**President Bush to Announce Cyber-Security Initiative.** On 9 May 2001, at Gartner's Spring Symposium in Denver, Colorado, Richard Clarke, Senior Director and Special Assistant to the President, who serves as the National Coordinator for Critical Infrastructure Protection, Counter Terrorism, and Security, announced that U.S.

---

President George W. Bush will order a new national plan to protect critical infrastructure. This plan will include the private sector in developing a consensus for a secure network architecture.

In making his announcement, Clarke said, "The President believes that cyber-security and critical infrastructure protection are essential to the national economy's health, are essential to the function of governance systems and are vital to the national security of the United States." The new initiative identifies cybercrime as a symptom of the problem. As the solution, the new administration proposes to develop, by at least 2004, a secure IP-based Supranet extending from the core national infrastructure to individual offices to the multitude of individual devices. The solution will incorporate recommendations from all major components of the nation's critical infrastructure, including the power grid, the banking systems, telecommunications and the transportation systems.

This policy initiative will enrich and strengthen the work begun under Presidential Decision Directive 63, issued in May 1998. The Directive requires that the executive branch of the U.S. government "assess the cyber-vulnerabilities of the Nation's critical infrastructures — information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health, as well as those authorities responsible for the continuity of federal, state and local governments." The Directive placed special emphasis on protection of the government's own critical assets from cyber-attack and the need to remedy deficiencies so that the government can become a model of information security.

Gartner has advocated an approach to protecting national infrastructure similar to that announced by the Bush administration. By involving the private sector in defining the information-sharing requirements and procedures, Gartner feels that the architecture for the Supranet will incorporate significantly improved audit, logging and diagnostic capabilities, which will ensure the trustworthiness of this crucial national infrastructure.

Analytical sources: William Malik and French Caldwell, Information Security Strategies

**Genesys' Acquisition of IBM's CallPath Will Allow Both to Focus.** On 11 May 2001, Alcatel announced that its subsidiary Genesys Telecommunications Laboratories plans to purchase the assets of IBM's CallPath assets. Genesys will acquire the software and hardware related to CallPath as well as IBM's development initiatives on next-generation unified communications and Java platforms. The vendors did not release the financial details, but Gartner expects the deal to close in June 2001 with no regulatory problems. Genesys will offer employment to IBM's 54 CallPath workers. IBM and Genesys have also agreed to jointly develop new contact center offerings that combine IBM's products for unassisted service with Genesys' for assisted service. Genesys and IBM will jointly market contact center solutions consisting of Genesys' Universal Queue Routing, Internet Contact Center and Outbound Solutions, and IBM's DirectTalk, WebSphere Voice Server and WebSphere Application Server.

With this move, IBM acknowledges that to remain competitive the CallPath platform required major enhancements in universal queuing and the integration of publicly switched telephone networks. In addition, the CallPath product created a conflict for IBM in non-CallPath call center environments. By divesting itself of the computer-telephony integration and universal queuing functions, IBM can now focus

---

## At Random (continued)

on DirectTalk and related WebSphere applications and infrastructure. Gartner expects that the deal will increase IBM's ability to operate in multiple call center environments. IBM Global Services will also benefit in having the opportunity to continue to work with IBM's CallPath customers, while expecting better access to Genesys' customers as well. Genesys will benefit in several ways, including: increased opportunities to become the migration path of choice for IBM's 400 CallPath customers; increased integration capabilities through IBM Global Services; and the gain of an experienced call center team.

Genesys has committed to continuing the IBM CallPath product for two years from the date of the finalized agreement and plans to offer a strong migration package. CallPath customers should continue to call their IBM contact for service until Genesys defines a new maintenance and support plan. Enterprises planning to purchase CallPath or planning major upgrades should consider putting these plans on hold until Genesys completes its migration plans. Enterprises can then evaluate these plans against competing migration offers from other vendors. For now, enterprises can start early planning for their eventual migration.

Analytical sources: Bernard Elliot and Drew Kraus, Enterprise Network Strategies

**Declining Demand for Hosting Services Presents an Opportunity for Enterprises.** On 9 May 2001, Exodus Communications, the leading independent provider of data hosting services in the United States, announced plans to reduce its workforce by 15 percent. Several other providers of hosting services, including Digital Island and Intel Online Services, have recently scaled back construction of data centers or taken other cost-reduction measures.

Gartner has long predicted a decline in the market for data hosting services due to massive overbuilding and overcapacity, and the recent downturn in the U.S. economy has accelerated that decline. Demand has dropped most among wholesale customers — application services providers, Internet service providers and Web hosters — that buy from providers such as Exodus and then sell to enterprises. Although overall demand is lower, the demand for full-service offerings is actually increasing.

In this saturated market, hosting services have become commodities, with little to differentiate one provider from another. Vendors often ignore one of the few differentiating factors — quality of service. Many providers have found it difficult to build constantly and still maintain acceptable service. Those providers that have built fewer — and frequently smaller — data centers offering more robust functions and better infrastructure have generally fared better than those that have focused on quantity at the expense of quality.

A few major providers, including AT&T and Sprint, have the resources and the experience to continue building aggressively, but few of their pure-play competitors will be able to do so. Many will have to seek partnerships with large bandwidth providers — e.g., telephone companies and online services — and network services providers.

---

Gartner believes that enterprises, which increasingly like hosting services, can benefit significantly from the decline in this market, especially since hosting service prices will likely fall 20 percent to 25 percent through 2003. Gartner recommends that an enterprise considering a hosting service provider first define its architecture requirements, inspect all aspects of the provider's infrastructure, ensure the provider's financial viability and assess whether the provider's competencies will mesh with its own architecture.

Analytical source: Ted Chamberlin, Enterprise Network Strategies

**Canon Withdraws From Monochrome Workgroup Printer Market.** On 30 April 2001, Canon stopped selling its monochrome workgroup laser printers in the United States. Canon re-entered direct sales and distribution of its workgroup laser printers in 1998. Now in an apparent reversal of that strategy, Canon told Gartner that it stopped selling its Canon-branded monochrome workgroup printers in the United States, effective 30 April 2001. A vast opportunity has eluded Canon: In 2000, two years after launch, its brand captured barely more than one-tenth of one percent of the \$1.9 billion spent on monochrome laser printers. Although Canon will still sell color laser printers under its own name, it represents a smaller (but growing) opportunity, with spending totaling only \$787 million in 2000. Canon will also redirect some of its resources back into its core copier products, which, of course, will still sell under the Canon brand name. (Canon's action does not affect its desktop printers sold through the retail channel.) Although Canon does not discuss contract business, Gartner also has no doubt that it will continue to manufacture workgroup printers for Hewlett-Packard (HP), which uses Canon as its primary print engine supplier. In fact, HP and Canon will now become even more dependent on one another.

Canon's withdrawal reflects the significant challenge that vendors face in building a two-tier distribution network to sell printers. Developing this kind of infrastructure can take years, and Gartner suspects that Canon underestimated the time and money required to grow such a channel. That, combined with poor sales and HP's continuing to do well in its sales of printers, probably made Canon's senior management reverse its course. At the same time, the overall output market will likely continue to move to a service focus — vendors will provide comprehensive output outsourcing services. Today, Canon depends on its distributors to provide these services. Its largest distributor, Ikon provides outsourcing services and also offers HP printers as part of its portfolio.

Enterprises evaluating Canon workgroup printers should make other plans. Canon has assured Gartner that it will continue to service and support the monochrome laser printers it sold under its own brand just as it would have done if they had not been withdrawn. Enterprises that have Canon printers should ensure that Canon will continue to service and support those products and should amend their service contracts to that effect.

Analytical sources: James Lundy, Ken Weilerstein and Don Dixon, Integrated Document & Output Management

# Has security, risk and privacy been on your mind lately?

June 11-13, 2001  
Orlando, Florida

**Gartner**

Join us at the 7<sup>th</sup> annual Information Security conference: **“Securing the Infocosm: Security, Privacy and Risk Management After e-Business”** and learn how to protect your company’s information.

#### **Key issues to be addressed:**

- What the “infocosm” is and how it affects security measures
- The best way to deal with privacy problems
- How to keep your environment manageable and secure
- Expectations from business partners, employees and regulatory officials
- Vendor offerings that help you protect valuable enterprise information
- Marketplace changes and how they affect the organization

#### **You’ll also benefit from:**

- One-on-Ones with Gartner analysts
- Networking with your colleagues

Register Today!

**Securing the Infocosm: Security, Privacy and Risk Management After e-Business**

**To register and for full conference details visit:**

**[www.gartner.com/infosec/usa](http://www.gartner.com/infosec/usa)**

**or call**

**1-800-778-1997 or +1-203-316-6757.**