

Gartner Says U.S. Businesses Must Make Privacy Management a Priority

Gartner to Address Privacy Issues at the Gartner IT Security Summit, June 2-4 in Washington D.C.

STAMFORD, CONN., May 19, 2003 — The need for privacy management is increasing and U.S. businesses must implement more robust customer privacy policies now or face government intervention and severe customer backlash, says Gartner, Inc. (NYSE: IT and ITB).

Gartner research shows that many U.S. citizens have accepted sacrificing some of their personal information privacy as a price for heightened security, but some businesses are taking advantage of those sacrifices and are using personal information for marketing purposes.

"Economic pressures are driving businesses to be more aggressive in how they address customers, but the privacy sacrifices that customers make for national security will not translate into tolerance for privacy abuses in less-critical areas, such as marketing," said Walter Janowski, research director for Gartner. "In a climate in which the general public is greatly concerned with corporate ethics and accountability, a business that makes a significant misstep in managing its customers' private information could face a highly visible and damaging public scandal."

Janowski added, "If U.S. businesses don't prioritize privacy management, public outcry will motivate the U.S. Congress to mandate restrictive privacy legislation." To ensure the privacy of consumers' personal information and avoid mandated government legislation, Gartner recommends that businesses do the following:

- Proceed with efforts to reinforce privacy programs by instituting formal processes to restrict internal access to personal customer data.
- Adopt proactive marketing techniques to solicit "opt-in" permission from customers for marketing.
- Consider U.S. government privacy regulations in the healthcare and financial services industries as indicators of possible general privacy regulations (Healthcare Information Portability and Accountability Act, or HIPAA, and USA PATRIOT Act, respectively). Also, consider new California legislation SB 1386 that will come into effect in on July 1, 2003 mandating that all entities conducting business in California through electronic means must report breaches of security which could effect California residents.
- Examine the rules and laws regarding privacy of the European Union and the Association of South East Asian Nations as possible templates for U.S. regulations.

"Although businesses and vendors cannot forecast the shape that U.S. government privacy legislation could take, those that address privacy management concerns today will be ahead of their competition and will be better prepared to accommodate privacy legislation requirements," said Janowski.

Another hurdle is that a majority of businesses are indifferent when it comes to purchasing vendor solutions for privacy management, and vendor interest is limited in delivering solutions.

"Businesses are hesitant to buy solutions until they are more compelling, but vendors are reluctant to devote resources to development until more customers are willing to buy," said Janowski. "Caught in the middle are customers who are confused and highly sensitive about the security of their personal information."