

TOP 10 TECHNOLOGY CONCERNS

CPAs have consistently recognized the potential for threats and opportunities for shielding individuals, organizations, and business and accounting professionals from attacks. The results of the AICPA 2006 Top Ten Technologies survey noted the following issues of greatest concern:

- **Information security:** the hardware, software, processes, and procedures in place to protect information systems from internal and external threats. They include routers, perimeter firewalls, IP strategy, intrusion detection and reporting, content filtering, antivirus, antispyware, password management, vulnerability assessment, patch management, personal firewalls, wireless security strategies, data encryption, locked facilities, and user education.
- **Assurance and compliance applications** (e.g., SOX section 404, enterprise risk management): collaboration and compliance tools that enable various stakeholders to monitor, document, assess, test, and report on compliance with specified controls.
- **Disaster and business continuity planning:** the development, monitoring, and updating of the process by which organizations plan for continuity of their business in the event of a loss of information resources due to theft, virus infection, weather damage, accidents, or other malicious destruction.
- **IT governance:** the structure of relationships and processes to direct the enterprise in order to achieve the enterprise's goals by adding value while still balancing risk versus return over IT and its processes.
- **Privacy management:** the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information. As more information and processes are being converted to a digital format, this information must be protected from unauthorized users and from unauthorized usage by those with access.
- **Digital identity and authentication technologies:** ways to ensure users are who they say they are. These include hardware and software solutions that enable the electronic verification of a user's identity or a message's validity through, for example, digital certificates. This technology includes the use of bar codes, magnetic stripe, biometrics, and tokens, as well as access control for authentication, nonrepudiation, and authorization.
- **Wireless technologies:** connectivity and transfer of data between devices via the airwaves (i.e., without physical connectivity). Wireless technologies include Bluetooth (PAN), infrared, WiFi (802.11 WLAN), WiMax (802.16), 2.5 G and 3G (WWAN), and satellite.
- **Application and data integration:** using current and emerging technologies, including .NET, web services, Java, XML (the foundation for XBRL), and Ajax, to facilitate integration of data between heterogeneous applications. In its most basic format, XBRL focuses on improving the gathering, analyzing, sharing, and synchronizing of business reporting data. This allows organizations to select "best of breed" applications that can be seamlessly integrated.
- **Paperless digital technologies:** document and content management, including the process of capturing, indexing, storing, retrieving, searching, and managing documents electronically (PDF and other formats), including database management. Knowledge management then brings structure and control to this information, allowing organizations to harness the intellectual capital in the underlying data.
- **Spyware detection and removal:** technology that detects and removes programs attempting to covertly gather and transmit confidential user information. Spyware applications are typically bundled as a hidden component of freeware or shareware programs, or attached to malicious websites. Once installed, spyware can monitor user activity, gather information about e-mail addresses, passwords, and credit card numbers in the background, then transmit the information to someone else. Spyware can include remote access trojans (RAT) and root kits.

Source: AICPA News Release: January 31, 2006; infotech.aicpa.org/Resources