

Envision the Future

Unleashing the Power of Converged Networks



State technology leaders across the nation are envisioning a future powered by Internet protocol and are quickly embracing IP products and services to enrich the lives of those living and working in the states. With state governments tapping the power of IP services at a rapid clip, network convergence is moving from theory to reality.

Convergence typically refers to taking historically separate voice and data networks and “converging” them into a single system to support IP-enabled devices such as phones, computers, cameras and applications yet to be conceived. Technology leaders in government and the private sector are embracing IP to streamline networks, control costs and introduce new communications tools.

As the work force becomes more mobile, convergence empowers governments and enterprises to extend their reach beyond the traditional four walls. Whether it’s a college campus updating from a legacy network to an IP network to facilitate distance learning or a state agency adopting video conferencing to keep up with agents in the field, network convergence changes how we conduct business in our daily lives.

The technology has finally caught up with the vision. Voice over IP (VoIP) calls no longer sound like two people talking through soup cans and a string. Technological

SURVEY RESULTS: NETWORK CONVERGENCE

Here’s one particularly interesting question — and the answers — from the 2008 *Digital States Survey*: What is your state’s readiness for migration to advanced communications platforms such as voice over Internet protocol (VoIP), or solutions that converge voice, data and video on wireless and wire line communications?

45% Convergence partially adopted and evaluating unified communications*

Plans to adopt in next three years **21%**

18% VoIP partially adopted

Convergence fully adopted and evaluating unified communications* **11%**

2.5% VoIP fully adopted and actively evaluating convergence

No current plans **2.5%**

* Unified communications is distinct from convergence; it’s real-time delivery of communications based on the preferred method and the location of the recipient (such as with instant messaging, telephony, video, e-mail, voicemail and text messaging).

DIGITAL STATES SURVEY

Verizon Business congratulates the winners of the 2008 *Digital States Survey* and the commitment to ongoing investment in new technologies.

advances have brought the quality of VoIP calls on par with traditional analog services. More importantly, IP transmits all information in digital form, creating opportunities for unified communications — the integration of fixed and mobile devices and applications.

As the lines between voice, video and data blur, visionary state leaders are redefining the business of government. Enterprises are moving from legacy networks to next-generation IP networks based on multiprotocol label switching (MPLS). These advanced networks meet new bandwidth demands and enable services such as hosted VoIP, private IP and managed services for years to come.



The technology has finally caught up with the vision. Voice over IP (VoIP) calls no longer sound like two people talking through soup cans and a string.

California technology leaders have embarked on a visionary path through CALNET II to deploy IP services to improve the experience for those who live and work in the Golden State. In Texas, through two new contracts — Information Technology Security Services and Managed Services for Information Technology — state leaders are putting the mechanics in place to make IP convergence through secure managed networks a reality in the Lone Star State.

Verizon Business, as an IP leader and network-based provider of integrated communications and computing solutions, is at the forefront of network convergence for businesses, agencies and educational institutions in the United States and around the globe. We stand ready to work with governments to develop and implement a comprehensive strategy to realize the full potential of IP to meet the demands of today — and those yet to come.

— *Steve Young, group president for corporate and government markets, Verizon Business*

For more information about how Verizon Business can support your e-government or communication needs, please visit www.verizonbusiness.com.



DATA BREACHES ANALYZED

You've seen the headlines about data security breaches. Now you can see the facts behind them. Verizon Business recently published the *2008 Data Breach Investigations Report*. The report involved four years of research, taking into account more than 500 forensic investigations of data breaches covering more than 230 million records. Experts analyzed hundreds of corporate breaches, including three of the five largest ones ever reported.

Numerous findings from the report underscore the importance of taking proper security measures to protect data. Nearly 90 percent of the breaches studied could have been avoided had reasonable security measures been in place.

Several factors contributed to the conclusion by researchers that most attacks could have been prevented. For 90 percent of known vulnerabilities exploited by hackers and malicious code, security patches were available many months prior to the attacks. Of the attacks studied, 83 percent were "not highly difficult" for the criminals.

Sixty-six percent of the breaches involved data that the victims did not know was on their systems. And 75 percent of breaches were not discovered by the victim; most breaches go undetected for a significant time and are eventually discovered by a third party.

Traditional security efforts have centered on controls around the network perimeter. But the researchers concluded that organizations must look deeper than that and pay more attention to the data itself.

More than ever, organizations are sharing data with other entities — business partners, contractors, temp workers and more. That's all the more reason to take security seriously; 39 percent of data breaches originated with business partners.

Especially in today's environment — with more converged networks, more devices being used, more sharing and a more mobile work force — organizations need to reconsider their security fundamentals.

The report detailed numerous recommendations for improving data security, and can be viewed in full at www.verizonbusiness.com/Solutions/security/risk/databreach.