

Demand for Security Solutions Expected to Grow Despite Broader Market Softness

a report by

Mark E Sanders

President, Wall Street Technology Association (WSTA)



Mark E Sanders is President of the Wall Street Technology Association (WSTA), and a member of the Institute of Electrical & Electronics Engineers (IEEE). He has over 20 years of executive management and network technology experience and has held management responsibility in diverse functional areas, including technology, sales, marketing, finance and operations. Prior to joining BevAccess, Mr Sanders was Senior Director and Chief Technologist for Merrill Lynch. During his seven-year tenure, he was responsible for the executive management and operations of all technology products and services for the Merrill Lynch user community within the US. His industry employment also includes Salomon Brothers, Inc., JP Morgan, Sun Microsystems, Inc. and Grumman Aerospace Corporation. Mr Sanders holds a BSEE from South Western University and an Executive MBA in finance and management from Dowling College.

What a difference a year makes. Just over a year ago, technology providers and enterprise customers were patting themselves on the back, the Y2K changeover having passed without incident. The market outlook for technology was better than ever, and enterprises ploughed confidently ahead with new initiatives such as wireless deployments and website enhancements. Analysts projected aggressive adoption rates of such technologies, and the technology sector worked itself into a state of heightened expectation.

As it turns out, adoption of emerging technologies has been thwarted on numerous fronts. For one, enterprises continue to struggle with an endemic lack of bandwidth and network capacity sufficient to support data-intensive applications such as wireless Web access. Wide-scale adoption of previously lauded technologies such as Web-enabled phones and Wireless Access Protocol (WAP) has faltered. Accordingly, the technology sector has adjusted expectations in the public arena of global markets, excess inventories having contributed to a broader economic downturn.

Enterprises in the US are taking an inventory of their own, assessing the soundness of planned technology initiatives. New technologies are of course a double-edged sword, providing opportunities for added revenues and cost savings, but requiring heavy capital expenditures to reap their reward. Technologies that fail to justify themselves early in the process will quickly become apparent as information technology (IT) managers look for ways of streamlining operations.

Most industry observers agree that 2001 will be a year of reckoning for technology vendors, enterprise customers and analysts who missed the mark with their projections. The coming months will see consolidation among technology providers, with the forces of natural selection leaving the strongest players intact when markets eventually stabilise.

Chief information officers at several leading US financial institutions only modestly scaled back their budgets for 2001, and e-commerce and Web

initiatives remain a top priority. For financial services, security products are part and parcel of Web initiatives, with touch points to the corporate backbone bringing heightened risk to the sector's most prized asset, its intellectual property and proprietary data. If such initiatives are undertaken, demand for security solutions could continue to grow in spite of softness in the broader technology markets. That, according to Bob Lam, senior network infrastructure and Internet security analyst at Bear Stearns, is because enterprises – not only financial institutions, but other large enterprises as well – will need security software and systems irrespective of whether they trim their overall spending.

Indeed, a January 2001 report says that new delivery channels for potential cyber-terrorist activity, such as wireless devices, will make online security breaches the most nefarious threat to businesses this year, with financial institutions among the most likely targets.

Of course, on the path to embracing the Internet, financial firms have long recognised the need to combat security risks online. Major financial institutions including Citicorp, Pershing and the Depository Trust Company (DTC), joined forces last year, forming the Financial Services Information Sharing and Analysis Center (FS/ISAC), which jointly reports on viruses and other potential threats in an anonymous online forum.

The industry's vulnerability became clear in 2000 when several high-profile security breaches seized the public's attention. For example, E*Trade fell victim amid a spate of cyber-attacks to large commercial websites in February 2000. A recent survey of security experts found that some 90% of Internet sites remain vulnerable to some form of attack via transactional server, 'buggy' software or internal code at the application layer.

Given such threats, financial businesses are relying increasingly on insurance companies to obtain e-risk coverage, and the market for e-risk insurance is gaining traction. Yet, such coverage provides little comfort to customers when their online security has been compromised.

Notwithstanding these concerns, Internet and wireless technologies are expected to proliferate in the coming years and it is predicted that one billion mobile devices will be in use worldwide by 2003.

To help enterprise customers extend their networks securely beyond the corporate firewall, security solutions providers have been working aggressively to enhance their products. For instance, the leading online security solutions providers have banded together to support XML, making it easier for developers to integrate applications with other multi-platform public key infrastructure products and services. In November 2000, a security network services provider introduced its XML Key Management Specification, which two of its rivals agreed to support.

Mobile phone manufacturers have also joined forces to develop a common framework for mobile e-business. Specifically, the framework provides a set of specifications that dictate how mobile transactions are processed. The specifications merge several existing mobile e-business initiatives to create a de facto standard for secure mobile e-business transactions. Ericsson, Motorola and Nokia have led the joint effort to unify e-business standards in partnership with representatives from leading financial institutions, telecoms providers and other industries.

A number of open forum security standards have evolved as well. For example, security improvements are available in the new release of WAP. Whereas the previous version made it possible to intercept a message as it passed between wireless and wired networks, WAP 1.2 uses digital certificates to add encryption between the wired-to-wireless network connection. WAP 2.0, which is also in the works, incorporates the Wireless Mark-up Language (WML) and eXtensible HTML (XHTML), enabling developers to build applications one time for multiple devices.

A large New York-based investment bank has set up dedicated leased lines to the firm's wireless provider networks to ensure that encryption is handled within the firm's firewalls. This bank will be deploying the new release of WAP to perform tasks such as tracking serial numbers of specific devices, personal identification numbers (PINs) and user passwords.

As for the Internet, security online has improved, but not at a level that business can be conducted anywhere in the world. The greatest security challenge financial enterprises face vis-à-vis the Internet is user authentication. Says one financial IT executive, "The Internet as a transport mechanism is

stable, but a browser can't authenticate the individual user. And there are no mature technologies that support the unique identification of browser users on a PC or other terminals on the network."

Financial organisations will address this challenge by using technologies like biometrics and smart cards. For example, Merrill Lynch began pilot testing smart cards last year and, in early March, RSA Security introduced a cryptographic smart card system that enables a single card to be programmed for network access, corporate identification and physical building access. It is easy to imagine financial employees, such as portfolio managers, using smart cards while travelling, to access the corporate network.

Ironically, exciting new technologies such as wireless Web access and smart cards make the more traditional policies and procedures more important than ever. With small form-factor devices, the risk of network intrusion rises sharply since they are easier to steal or misplace. When introducing new distributed devices to the enterprise network, financial firms must establish and enforce stringent policies to manage network security. For example, many firms have designed 'kill features' that are immediately triggered when a wireless device is lost or stolen, shielding the network from intruders and eliminating access to information on the device.

While the challenges with emerging technologies remain, so do the opportunities they provide for enabling enterprises to find better ways of conducting business. Yet, the continued proliferation of e-business and wireless technologies places greater responsibility on IT managers, particularly in financial services, to carefully integrate the new technologies. Simon Blake-Wilson, Research Director of Certicom, says that financial firms must architect their security policies as carefully as they craft the network security infrastructure itself. "As more applications come online, enterprises will need to perform careful analysis of their security requirements, and on-going management of this will be key," added Blake-Wilson.

In hindsight, 2001 may be sobering in contrast to 2000, but that is not necessarily a bad thing. As an industry, we now have the opportunity to reflect on the previous year, reassess our projections and adopt the most effective technologies moving forward. Enterprises that seize the opportunity will be best equipped to assess new innovations and opportunities as they arise, as more is learned during challenging times than any other. Likewise, successful enterprises will leverage this uncertain climate to test their strengths, sharpen their core competencies and prove their ability to adapt in an ever-changing economy. ■