

# One Tough Customer

Want to sell more data services to enterprise customers? Former Citigroup Security Czar Steve Katz tells you how.

By Steve Goodwin

Seeking meaningful gains in productivity, efficiency and customer loyalty, business enterprises around the world are "going wireless" in record numbers. And network operators are responding. They are now offering enterprises a growing variety of wireless data services, realizing an unprecedented opportunity to increase revenues and leverage their existing infrastructures.

At first glance, it seems like a match made in heaven, and the financial projections certainly support that notion: network operators' revenues from wireless data services are estimated to reach \$50 billion in 2006 and grow to more than \$90 billion in 2008.<sup>1</sup>

However, an increased awareness of potential wireless security issues among enterprise customers – fueled by well-publicized reports of costly incidents – threatens to cast a long shadow on this otherwise bright vision of a wireless future. How great are the security concerns of enterprise customers served by wireless operators? In a recent industry survey, most respondents clearly stated that they would invest more in mobile technology if these security concerns were addressed.<sup>2</sup>

To help network operators better understand the security hurdles they must overcome in selling wireless data services to enterprise customers, Motorola Wireless Security Services (MWSS) sat down with Steve Katz, CISSP. Former Chief Information Security Officer at J.P. Morgan, Citigroup and Merrill Lynch. Katz is a noted speaker and author and the founder of Security Risk Solutions. Among his many duties as CISO, Katz was charged with evaluating the security of the wireless data communications services offered by network operators. Here, he



Former Citigroup, J.P. Morgan and Merrill Lynch Chief Information Security Officer Stephen R. Katz, CISSP

## Wireless Data Services: The Market and The Challenges

- **The Buyers:** Enterprises looking to improve productivity, efficiency and customer service and extend corporate networks to mobile and remote workers.
- **The Sellers:** Network operators seeking to create new revenue-generating service offerings while leveraging their current infrastructure investments.
- **The Challenges:** Heightened security awareness, strict regulatory requirements and the potential for irreparable brand damage have led enterprises to demand increased, verifiable security features and measures from the network operators proposing to sell them wireless data services.
- **The Solution:** Network operators must meet enterprise customers' security demands head-on and demonstrate that they have taken a proactive, customer-centric approach to wireless security.

once again plays the role of a tough customer armed with a number of tough questions for network operators.

**MWSS: What are the top security concerns a carrier must address in order for you to consider purchasing its wireless data services?**

**Katz:** As a potential customer, my top concerns will be driven by the type of service being proposed by the carrier. Will they just be serving as a pass-through, not providing any applications or storing any of my sensitive corporate data? If this is the case, then I look for a carrier to ensure that my logon information is encrypted from the instant it leaves my device through to establishing a VPN connection. I'll also want the carrier to demonstrate some unspoofable means of authenticating the device itself. Before that VPN connection is established, the device or laptop should talk to the carrier to say, "I really am who I say I am, and I belong here."

If the network operator would be providing applications and/or storing my data, it's a whole different ballgame with significantly more hurdles to clear. Now they need to demonstrate their compliance with industry-accepted security standards, such as ISO17799 2005. In the financial world, I'll be looking for the operator to establish that they are in full compliance with the requirements of the Gramm-Leach-Bliley Act of 1999 (GLBA) and can pass a Federal Financial Institution Examining Council (FFIEC) Handbook for Security audit. If I'm in the healthcare industry, I want the carrier to demonstrate compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). There are also a number of state privacy laws requiring companies (and their service providers) to notify any party whose data is potentially compromised in the event of a security breach. Of course, if my company is a multi-national organization, then I'll want to know that the operator is in full compliance with the applicable laws of the countries in which I do business. One example would be the European Union Data Protection Directive. Japan, Argentina, Canada and virtually every other country have similar laws, nearly all of which are more stringent than those in effect in the U.S.

And it goes beyond merely complying with these regulations and statutes. Before I consider buying wireless data service, I need to know that the operator's information security program and compliance with applicable regulations has been audited by a reputable third party who really understands security. I also need to know that the operator has an on-going certification process in place to ensure it remains in compliance.

In nearly every industry, reputation is everything. As the enterprise, it's *my* reputation that's at stake if the network operator experiences a security breach. If employees cannot connect securely to critical systems, or if customers have confidential information stolen, they're coming straight to *me*, not to my carrier.

Today, network operators are hosting simple applications for the consumer market that range from ring-tones to wallpaper. But, they are expanding applications to serve the enterprise market to include transaction-based services, hosting of mobile workforce applications, and multimedia applications. When selecting a

"The first operator that stands up and makes the strong case for security is the one that everyone else will need to catch."

carrier to provide wireless data applications, it's imperative for enterprises to remember that although they may be giving up operation of the application, they cannot – and do not – give up responsibility for the security, confidentiality and integrity of the information.

**MWSS: What are some of the security considerations typically overlooked by enterprises considering purchasing wireless data services?**

**Katz:** Some enterprise buyers have been misled into thinking that having a VPN is the total answer to all of their wireless data security problems. In reality, it's just the first step. At the very least, enterprise customers need to have full, end-to-end encryption in place.

Another common mistake is to forget that security goes hand-in-hand with reliability and availability. When dealing with a network operator, you need to make sure that they're "always there." If you have end-of-quarter deadlines and need to send large chunks of data across the wireless network, you need to know that the operator has not only secure bandwidth, but also sufficient and reliable bandwidth as well as the staff ready to help you should an incident occur. At that point, reliability and availability become every bit as crucial as security when customers evaluate an operator's overall Quality of Service.

**MWSS: What are some of the "must-have" security features/controls that enterprises look for when choosing a wireless data services provider?**

**Katz:** In addition to compliance and adherence to applicable regulations and industry-accepted best practices, I also want to know what controls the operator has put in place over people, policy, process and technology. Do they train their staff in security? Do they have their own internal, comprehensive security audits, standards and guidelines? Is security ingrained in their operations? Before I even consider signing on, I need to know that the operator has the right answers to these and other questions. I need to know that they can ensure the integrity, confidentiality and security of the information – *my* information – that transits their network.

As corporate customers become increasingly dependent on third-party networks for enterprise mobility applications, the impact of security on network availability is critical. As a result, I want to know, in great detail, about the totality of the operator's security practices. This, of course, would include how they handle vulnerability and patch management issues as well as how they deal with worms, viruses, trojans and other malicious attacks that affect both availability *and* security.

Once you entrust your data to a wireless operator, that operator becomes an extension of your company's brand. And whichever operator you choose *must* get a clear message: any event that could impact my brand will cause me to take my business elsewhere.

**MWSS: What's the biggest security-related mistake a carrier can make when trying to sell you wireless data services?**

**Katz:** Wow! There are a lot of mistakes that are made all the time, from overstating

"If someone is trying to sell me wireless data services and they go five minutes without talking about security, availability and reliability, then they don't make it to the sixth minute."

potential benefits to not understanding my business. But, the biggest mistake a carrier can make is not adequately addressing security and trust requirements as they pertain to my business. If someone is trying to sell me wireless data services and they go five minutes without talking about security, availability and reliability, then they don't make it to the sixth minute.

If a carrier won't submit to a rigorous third-party assessment that includes – at the very least – an attack and penetration test or “ethical hack,” then that's a deal breaker. If you can't stand up and say that you've been audited and are in compliance, then leave my office.

**MWSS: What are the key security measures that a company should have in place before purchasing wireless data services?**

**Katz:** From a security perspective, it's critically important to have your own house in order before you implement any new technology, particularly outsourced wireless technology.

Enterprise customers must have full, end-to-end encryption and a tested and validated VPN. You'll also need to prove that you have effective authentication at your site, so when the connection is made, you can verify unique characteristics of the user's device. This would include the use of tokens as well as ID/password and endpoint security checks on the devices coming in.

Companies purchasing wireless services must also establish and implement internal security policies and monitor and measure employee adherence to those policies. For instance, you'll want to make sure that your road warriors know that having wireless access is a privilege, not a right: they have to demonstrate a valid need for wireless access and show that they are adhering to company policies regarding its secure use.

**MWSS: What is the current state of security among network operators and where do they need to be in order to sell more wireless data services to enterprise customers?**

**Katz:** In preparing for this interview, it didn't surprise me to see that very few network operators – even the biggest players – are talking openly about security on their web sites or in their service literature. If there's currently a “security movement” among wireless data service providers, it's one of the best-kept secrets in the industry.

Network operators need to lead with security. They need to turn security into a key differentiator, particularly when trying to sell wireless data services to companies in security-sensitive and highly regulated industries. They need to demonstrate that security is part of the fiber of their being and is an integral part of their service offerings – in place and verified.

There are a number of steps that network operators can take. First, they'll want to find a highly regarded, expert security partner who understands the role that security plays in facilitating a trustworthy data-networking environment. Going beyond perimeter defense, this partner can help an operator create the comprehensive wireless security strategies and programs that ensure their network is designed to

“If there's currently a ‘security movement’ among wireless data service providers, it's one of the best-kept secrets in the industry.”

be secure from the ground up. Once these strategies and programs are in place, the security partner should conduct a rigorous third-party assessment, allowing the operator to demonstrate to both subscribers and prospects its proactive security approach.

Operators will also need to adopt a holistic view of security that considers people, process and policies in addition to technology. Additionally, they need to implement security training programs for all internal staff and make certain that their sales teams are well-versed in their security processes and practices. Finally, these companies need boost their security profiles by becoming active in industry security forums and associations.

Look at the financial services industry: security is an integral part of what they do. They talk to their customers about security right up front. And their security practices are highly regulated. It's becoming largely the same in healthcare. It's time for network operators to follow those examples. The first operator that stands up and makes the strong case for security is the one that everyone else will need to catch.

<sup>1</sup> Motorola Network/Industry Research and Analysis.

<sup>2</sup> Survey of attendees at the 2005 CTIA (Cellular Telecommunications Industry Association) Wireless IT and Entertainment conference conducted by Bluefire Security Technologies, Inc.