

“Security Upstream: Where Users Turn to Their Service Infrastructure”

Gone are the days of safety by mere desktop antivirus protection. Practically every smart device, whether a PDA or the mobile handset, is under fire by the pervasive threat of viruses and the vulnerability to hacktivism. And the battle is far from being won as technology users throw their hands up in the air and turn to their service providers for solutions. Many subscribers have made the assertion that network carriers are somehow responsible for furthering this socio-technology malaise, but reality says no one method of protection is really quite good enough.

So, if firewalls and personal software protection aren't the only combination to tackle intrusion, then why not look upstream for the answer? A popular method invoked by virtual email servers such as Yahoo! that began with managing spam and simple virus infections appears to be gaining adoption in the broader service provider sense. By ratcheting up security at the network point of entry and offering failsafe filtering down to the individual, the elimination of virus propagation and targeted attacks seems to be working. Barriers put in place to stop the attack in the background before ever reaching the device-level presence offer some smart economics. Service providers win by less customer complaints, and customers in turn realize higher productivity from their infrastructure investments.

An ongoing study launched in 1999 between our firm and a coalition of university academics has identified the cost of network intrusion to be far greater than the actual costs of data and restoration processes. Rather, the real impact is quantifiable in terms of lost revenue and productivity to those fateful to encounter network breach. On average, annualized losses are now showing comparable to 6.42% of a company's adjusted gross revenue, up nominally from 5.97% just two years ago. Albeit, while more dollars have been poured into enterprise security firmware, the performance remains somewhat stymied in comparison to the escalation of attacks.

This hints toward the notion of looking at the network infrastructure holistically, not as starting at the premises but rather a total span of interconnectivity, including mobile data and wireless access. Every point at which a subscriber touches the network becomes a junction for examining security practices. And this means that service providers must sharpen their edge on handling threats before their customer's network is subject to attack.

Massachusetts-based Quarry Technologies (www.quarrytech.com) recognizes the value carriers must convey to their VPN (virtual private network) customers in order to ensure network stability. Quarry's director of marketing, Greg Whelan, describes the proposition of upstream network security as a pivotal point of service differentiation. "Secure networks translate to an infrastructure that has customer productivity in mind, with assurance that integrity is maintained across points of access beyond the subscriber's enterprise," notes Whelan. For top-tier carriers, security starts in framing their service level agreements and ensuring continuity throughout the service period. And to a larger degree, customers have wised up to asking for such assurances as part of their enrollment terms.

With so much at risk for both service providers and their customers, the elusive question is how much in terms of security resources should be spent to solve the problem of active and passive intrusion attacks. And as attempts to thwart countermeasures increase, does the carrier have any other choice but to curb hacker penetration at the source? The obvious conclusion is to fortify the well to prevent poisoning downstream, but until network providers can equate dollars to customer loss, the point may not be so clear.

