

“A Rising Tide for Network Security”

First there were viruses—and then came the worms. Now, intrusion of networks and servers seems to be child play in a game of cyber-terrorism that has wreaked havoc for millions around the globe. Last week’s attack by the ‘Slammer’ worm only heightened the security senses of the ill prepared and set a stake in the ground against the anticipation of next-generation hactivism. And the sobering reality set in after the apparent economic devastation shutdown the commerce capabilities of airlines, banks, and trading exchanges—not to mention tens of thousands of users unable to access their email accounts.

Digital society as we know it today is stumbling upon a rude awakening. Security is no longer squarely concerned with the obvious threats of credit card fraud, identity theft, or even rogue counterfeit scams. Yes, the problem is rooted deeply in the all-too-real escalation of malicious hacking and attacks aimed at disabling the network community at large and keeping them from going about their normal mode of business. Hactivism—and its social malaise of senseless destruction—has taken on new meaning to network subscribers and the information assets that they seek to protect.

On the heels of such prominent incidents, Cisco Systems announced their intent to acquire Okena Corporation (Waltham, MA), a developer of network security software that acts as a vanguard against system hacks before they occur. For the exchange of \$154 million in common stock, Cisco furthered the consolidation trend of vendors in this market and gained a strategic foothold in protection of endpoint devices—namely those servers and users left vulnerable at the edge of authentication and access. Using technology that preempts a hacker’s destructive intrusion, the security approach operates transparent to the authenticated user but effectively halts any damage to operating system files or applications before a breach exists. As the end-to-end network becomes more susceptible to hosted applications and the like, system administrators find themselves battling to not only regain control of the user environment but also those seeking access by hacktivist means.

But the surge in network security pressure is more than just the threat of breach as corporate gatekeepers learn the relevance of risk mitigation. For every attack, there is an associated economic consequence—a loss of productivity, an erosion of customer confidence, or plainly a lack of efficiency in extinguishing the flames. Risk is an element that no network user or organization can mitigate 100% of the time since the vulnerabilities are endless and the innovation for loopholes to security outpaces the inoculation capabilities of vendors. Staying a step ahead works in theory, but is a minimalist strategy at best—given that hackers thrive on ways to circumvent the most sophisticated methods publicly known. Rather, it is better to consider lowering the risk quotient through a proactive assessment of weaknesses and implementing a recovery plan to ensure continuity of operations. And of course, the agents of network security deliver a healthy dosage of assurance to facing the inevitable.

Carriers themselves continue to master the concept of network reliability as proven well in recent decades, but even today’s breed of hacker behavior leaves the most secure networks at risk for compromise. And when it happens, the strike makes headline news. Disconnected customers and violated companies feel the pain all too well, and ultimately, the network itself is left to blame. There’s no greater lesson than an ounce of assertive

prevention is worth its weight in keeping out of harm's way. And judgment withheld, users expect their service providers to go the extra mile to preserve their access reliability and safety.

Hactivism is swelling at a rate that baffles our ability to control the network in a predictive order. Allowing hactivism to ruin the strides of marked progress in open connectivity, on the other hand, is a choice left in the service provider's court. Decisions made in advance to plan for risk and act sensibly is a wise move—before the next tsunami comes ashore.

