

### *Top-of-Mind Security Topics from the 2007 RSA Conference and Beyond*

#### **Most Discussed Market Opportunities**

**Data Security** – High-profile data thefts at TJX, Veteran Affairs and elsewhere have made data security a major industry topic and rapidly increasing focus area among enterprises. Complementary approaches have arisen to address the dangers, including locking-down databases, encrypting data and preventing information leakage. NAC and IAM (below) also play a key role by limiting who and what can access information.

**Endpoint Protection/Network Access Control (NAC)** – Laptops, flash drives, Blackberrys and other remote devices connecting to corporate networks can introduce viruses and enable data theft. Endpoint protection enforces configuration, patching and malware scanning policies to prevent infection. NAC also provisions rights and monitors access to prevent unauthorized usage. Numerous vendors announced products at the RSA Conference. Microsoft's Network Address Protection (NAP) framework and Cisco's NAC program already have over 100 partners.

**Identity and Access Management (IAM)** – FFIEC authentication guidelines for banks, HIPAA rules for healthcare and other compliance mandates regarding network integrity and data privacy have made IAM the fastest growing major IT security sector. IAM governs user authentication and access rights. Growth areas within IAM include single sign-on, credential management and strong authentication. All the major public infrastructure vendors – CA, EMC, HP, IBM, Oracle –have IAM offerings and seek gap-filling technologies. In their keynote RSA addresses, Microsoft chairman Bill Gates and chief strategy officer Craig Mundie discussed plans to phase out passwords in favor of certificate and hardware-based strong authentication. IAM complements and, over time, will likely converge with NAC.

#### **Most Notable Statement**

**In his RSA Conference keynote, RSA head Art Coviello predicted the demise of independent security vendors within 2-3 years** – While symbolically significant, this assertion by the host of the world's largest gathering of independent security vendors is premature. Unquestionably, pockets of overinvestment exist and consolidation is accelerating (see discussion below). However, many private security vendors enjoy material, rapidly growing revenues and stand to benefit from consolidation, which reduces

competition and strengthens pricing. Further, IT evolution drives continual change to the threat landscape, requiring innovations that have previously often come from smaller specialty vendors. Finally, surveys indicate that enterprises are still willing to pay up for the best security solutions; bigger does not always equal better.

#### **Most Observed Trend**

**Consolidation is Accelerating** – Large deals, including EMC's recent acquisition of RSA, are generating pervasive discussion about M&A's impact on the industry. Most observers agree that consolidation is accelerating. Evidence supports this: according to Udata research, 2006 security M&A volume rose 55% over 2005, to \$6.8 billion, and 2007 is already on pace to exceed 2006. At the same time, security venture investment volume declined 33% in 2006 to \$800 million. Large infrastructure vendors are the primary beneficiaries of consolidation. A recent Morgan Stanley survey found that Microsoft and Cisco are gaining spending share at 5-10 times as many enterprises as other major security vendors. Since January 2005 (prior to the Q1 2007 stock market dip), pure-play security stocks declined an average of 21% while the share prices of large, acquisitive infrastructure vendors rose an average of 32%. Currently, Symantec, McAfee and Check Point trade at discounts to mean cash flow multiples for the overall software industry. Notwithstanding pressure on pure-plays, ample opportunities (discussed below) remain for specialists. Additionally, disappearance of pure plays will take time – e.g., nine months after launching its OneCare security bundle, Microsoft still represents only 2-3% of threat management spending.

#### **Most Commented Upon M&A Transactions**

**EMC acquisition of RSA** – In June 2006 EMC announced it would acquire RSA for \$2.1 billion in cash, at a transaction value/trailing revenue multiple of 6.5x. In addition to being the largest deal of the year, RSA gives EMC a leading position in IAM and data security, threatening other stack dominators.

**Symantec acquisition of Altiris** – In January 2007 Symantec announced it would acquire Altiris, a public Microsoft competitor in desktop configuration, deployment and security management, for \$830 million in cash, at a

transaction value/trailing revenue multiple of 3.1x. The deal gives Symantec better control over enterprise desktops and makes it a more direct competitor to Microsoft. Altiris itself has been acquisitive, completing four M&A deals since 2004.

**Cisco acquisition of IronPort** –In January 2007, Cisco announced the acquisition of IronPort, a major provider of anti-spam appliances, for \$830 million, representing a transaction multiple of 8.3x trailing revenues. The deal brings Cisco squarely into threat management, at an eyebrow-raising price.

**Check Point acquisition of ProtectData** – In November 2006, Check Point announced it would acquire public Swedish data encryption vendor Data Protect for \$607 million, representing a transaction multiple of 9.2x trailing revenues. This acquisition is expected to help jump-start Check Point’s growth.

**Check Point acquisition of NFR** – In December 2006, Check Point acquired NFR Security, a small intrusion detection and prevention software vendor, for \$20 million. This deal is notable as a substitute for Check Point’s attempted SourceFire acquisition in 2005 for \$225 million, which was quashed by U.S. regulators. This “small is beautiful” deal is a reminder that, in security, size often does not always matter.

**IBM acquisition of Internet Security** – In August 2006, IBM announced it would acquire publicly traded Internet Security (“ISS”), the leading intrusion prevention vendor and a major managed security player, at a transaction value of \$1.1 billion –3.2x trailing revenues. The deal has increased pressure on HP and other leading infrastructure vendors to make bigger security bets. It is also notable that, despite representing a modest fraction of ISS’s total revenues, IBM presented managed security as a key driver for the transaction.

**Other Highlighted Opportunities in Security**

Despite industry maturation, promising niches offer outsized growth and valuation opportunities. Those receiving significant attention include:

**In-the Clouds/On-demand Security** – Although constituting a small fraction of security spend today, browser-based security services will ultimately become commonplace, particularly among SMBs and consumers. On-demand’s appeal lies in its simplicity: security functions are performed on internet traffic before reaching the network or user. Increasingly, ISPs and telcos are bundling security services with connectivity. On-demand in a sense competes with multi-function appliances (UTMs), because both offer multiple functions at lower cost and complexity. According to a recent IBM ISS poll, 41% of telco carriers said in-the-cloud services will be a major revenue generator for them within three years and 78% within five years.

**Physical-IT Convergence** – According to IDC, 10-12% of system integration engagements involve both physical and IT security. This is driven partly by unification of functions onto the network, e.g. IP-enabled surveillance. Other convergence opportunities include analytics and access control. Several dozen vendors on the RSA exhibit floor presented convergence offerings, a significantly greater number than the prior year.

**Mobile Security** – Encryption and threat management solutions are needed to address the security needs of –and threats posed by –an increasingly mobile internet user population. IDC predicts that, by 2009, 25% of the global workforce will be mobile networked workers. There has already been a steep rise in virus outbreaks targeting major mobile operating systems (Symbian, Microsoft, Palm) and data theft through compromised/stolen devices. This segment overlaps multiple areas including NAC and data security.

**Threat Management 2.0** – Antivirus and anti-spyware solutions remain largely signature-driven, and as such are inherently reactive and incomplete. The rise of zero-day exploits and the sheer number of new malicious code variants and infection vectors require supplemental approaches. Reputational, behavioral and policy-based technologies offer added protection; however earlier solutions have suffered from high latency and/or low accuracy. McAfee’s acquisition of early-stage SiteAdvisor, a web exploit prevention vendor, for more than \$70 million highlights the value of new approaches to malware, security’s oldest problem.

**VoIP Security** – A recent IBM-ISS survey of carriers found that security issues are impeding roll out of triple-play (voice, video and data) and “Quad-Play”(voice, video, data and wireless) service. 78% said security is vital to the long-term viability of VoIP service. Security vulnerabilities affecting computer networks equally affect VoIP systems and represent tremendous opportunities, both for established and new vendors.

###

[www.update.com](http://www.update.com)