

# FINANCIAL IT SECURITY

December 2006

Securing Financial Enterprises from the Inside Out

# THE FUTURE NOW LIST

BY REBECCA SAUSNER,  
MICHAEL SISK, MICHAEL  
DUMIAK AND HOLLY SRAEEL



## WHEN TALKING SECURITY IN 2006—AND, REALLY, WHO WAS-

**NT?**—two movements dominated the industry: authentication and consolidation. Thanks to proactive moves by the FFIEC, authentication became priority number one last October, triggering a spending spree by financial institutions that, Y2K aside, had many corporate officers blanching. That

two-factor authentication was mandated by year-end was bad enough, but companies also had to foot the bill for rigorous compliance spending. Security, it seems, comes at a price: Institutions were expected to spend \$700 million to \$1 billion on anti-fraud technology this year, according to Fortent, an enterprise risk management technology provider.

The urgency of security in financial services is also creating new job opportunities, and prompting institutions to rethink security roles. In 2006, there were an estimated 1.5 million IT security professionals worldwide, an increase of 8.1 percent over last year. That number is expected to hit two million by 2010. The demand for expertise can be spotted in what IDC says are the top areas for additional IT security training in the Americas: information security risk management, forensics and application development. “The traditional corporate security organization is less involved in day-to-day compliance activities; they’re not the one with the hammer anymore,” says Jon Dar-

byshire, CEO of Archer. “Business people have to either accept or not accept risk, and that information is being reported back up through the governance group [and] audit committee—that’s who has the hammer now.”

Some would argue otherwise. The game-changing rules dispensed by Washington had dramatic effects not only on financial institutions, but also on vendors, hastening consolidation from more than a dozen companies to a handful of credible players. Some of the largest deals of the year were EMC’s buy of RSA Security for \$2.1 billion and IBM’s purchase of ISS for \$1.3 billion. Other notables include Viisage and Identix’s biometric merger, estimated at \$770 million, and Secure-Computing’s acquisition of CipherTrust for \$273 million. No M&A discussion is complete without discussing Symantec, which bought IM Logic and Relicore this year, and has been on a buying binge since 2004, acquiring 10 companies, including Veritas for \$13.5 billion in 2005.

Consolidation has not been limited to the authentication space. Managed security service providers saw a good number of their brethren snapped up, while many point solutions were bought in the hopes of coming up with more advanced and integrated offerings to capture the imagination, and dwindling budgets, of chief information security officers—many expected to do more with less in 2007. “The security budget sometimes touched 10 percent of an organization’s overall IT spend,” says Khalid Kark, senior analyst at Forrester. “Those days are gone, and security managers now face decreasing budgets and increasing expectations from executive management.”

It is apparent that data needs security, and preferably encryption, wherever it travels. With CISOs fed up with managing too many point solutions that can’t be integrated, companies such as BT and IBM sought out Counterpane and ISS, respectively, to round out their security portfolios and provide CISOs with one-stop shopping capabilities. Smaller MSSP deals came with the merger of Lurhq and SecureWorks, and SurfControl buying BlackSpider to become one of the first content-filtering companies to offer its services any way customers want to buy them. “The days of standalone security companies are dead,” maintains Ross Brown of eEye Digital Security.

Yet budget constraints—security is pegged at nearly 8 percent of an institution’s overall IT spend in ’06—do little to sway expectations in the executive suite. And public awareness of fraud and information security threats grows stronger with every data breach and identity theft case reported. This leaves financial institutions in search of technologies and providers that will enable them to comply with state and federal data privacy and loss reporting regulations, while also meeting the stronger authentication mandate. But it also has institutions looking for technology that will extend protection beyond their perimeters—whether physical or virtual—to the laptops and data centers of vendors and their subcontractors. The long-term agenda for institutions is on identifying and implementing solutions that embed rights, access privileges and authentication into the workflow processes, systems, devices and partnerships related to information management. Pro-

gressive institutions are using security as a springboard to protect and enhance the equity of their intellectual property and information firmwide.

To this end, *Financial IT Security* has compiled its “Future Now List,” the first-annual ranking of the 25 best security innovations for 2007. Of the companies chosen, one thread is consistent: the technological sophistication of the products is so significant as to dramatically improve the enterprise’s ability to secure its data and devices going forward, while changing the way businesses manage information, internally and externally. Whether it’s EMC’s acquisition of RSA, Symantec’s partnership with VeriSign, or Liquid Machine’s machinations in enterprise rights management, the critical mission of information security is in protecting and managing data—wherever it resides or is being used.

Also included in this year’s ranking are Fortify/Watchfire, Archer, CyberTrust, PortAuthority Technologies, Imperva, Trend Micro, eEye, MarkMonitor, SkyBox, 3VR, AirMagnet, PGP, Secured eMail, RedSeal, BigFix, 41st Parameter, Secuware, nCircle, ArcSight, AXS-One, Incard Technologies and MessageLabs.

# 2006

## TOP RANKINGS

Javelin rates banks based on how well they protect their customers from identity theft. Overall rankings are out of 100 points. Detection scores, out of 35, indicate how easily customers can detect fraud. Prevention scores, out of 45, refer to proactive steps to prevent ID theft.

### »»OVERALL

- 80 »» BANK OF AMERICA
- 79 »» JPMORGAN CHASE
- 77 »» WASHINGTON MUTUAL
- 73 »» KEYBANK
- 64 »» FIFTH THIRD BANK
- 64 »» WELLS FARGO
- 63 »» MARSHALL & IISLEY
- 61 »» SUNTRUST
- 60 »» CITIBANK
- 53 »» MEAN

### »»DETECTION

- 35 »» JPMORGAN CHASE
- 32 »» BANK OF AMERICA
- 32 »» KEYBANK
- 23 »» CITIBANK
- 23 »» SUNTRUST
- 23 »» WACHOVIA
- 23 »» WASHINGTON MUTUAL
- 20 »» FIFTH THIRD BANK
- 20 »» PNC BANK
- 20 »» WELLS FARGO
- 18 »» MEAN

### »»PREVENTION

- 34 »» MARSHALL & IISLEY
- 34 »» WASHINGTON MUTUAL
- 33 »» BANK OF AMERICA
- 29 »» FIFTH THIRD BANK
- 29 »» JPMORGAN CHASE
- 29 »» NAVY FCU
- 29 »» REGIONS BANK
- 29 »» WELLS FARGO
- 26 »» KEYBANK
- 26 »» NETBANK
- 22 »» MEAN

### »»TOP IT SECURITY PRIORITIES FOR 2006\*

- 50% »» MULTI-FACTOR AUTHENTICATION
- 42% »» DATA ENCRYPTION/ PROTECTION
- 42% »» INTERNAL SECURITY PERMISSIONS
- 33% »» WIRELESS SUPPORT
- 17% »» COMBATING PHISHING
- 17% »» VENDOR RISK ASSESSMENT
- 17% »» AWARENESS/EDUCATION

# FIVE


## Archer's Customers Ask for Vendor Management and SOX Reporting Tools; As Usual, Archer Technologies Delivers

**CATEGORY:** COMPLIANCE **PRODUCT:** VENDOR MANAGEMENT AND SOX COMPLIANCE MODULES. **CLAIM TO FAME:** WORKS WITH 29 OF THE TOP U.S. 30 BANKS **WHAT'S AHEAD:** USERS ARE ASKING FOR ENHANCED RISK ASSESSMENTS AND THE ABILITY TO COLLECT DATA ONCE, AND USE IT WHEREVER IT'S NEEDED

» **ONE OF THE GREAT THINGS** about Archer Technologies is that it bases new product development decisions entirely on customer demand, as collected through its frequent user group conferences. And with 29 of the top 30 financial institutions as customers, six-year-old Archer Technologies has its product development team connected to the pulse of the industry. So, it's not too surprising that this year the company found demand for vendor management and SOX compliance modules were top priorities for its keystone customers. The vendor management product creates a central portal for all vendor compliance information, and automates risk assessments, contract reviews and ongoing monitoring. It's not as if customers weren't doing these assessments already, but most lacked a sophisticated system to dynamically track them, including workflow and action items. "Now we have customers that have as many as 10 assessments per vendor," says CEO Jon Darbyshire. "They want to be able to assess once and use that data many times."

Similarly, the SOX Compliance Management module enables institutions to utilize data that already resides in the Archer Technologies system for compliance, data aggregation, process control and reporting. Archer Technologies claims using its SOX compliance module immediately reduces the cost of compliance initiatives and allows the process to be easily duplicated. Archer's latest release also incorporates COBIT 4.0 and PCI standards.

Jim Routh, CISO at the Depository Trust & Clearing Corporation, says using Archer's vendor management portal drastically reduces the time he and his staff spend working with auditors and regulators to answer audit queries. Those costs can add up, given that auditors visit DTCC almost weekly. On a recent occasion, Routh says, more than 80 percent of the information needed was instantly available in the company's Archer Technologies security portal. (rs)

- 
- 01 » RSA
  - 02 » LIQUID MACHINES
  - 03 » SYMANTEC
  - 04 » FORTIFY/WATCHFIRE
  - 05 » ARCHER TECHNOLOGIES
  - 06 » CYBERTRUST
  - 07 » PORTAUTHORITY
  - 08 » IMPERVA
  - 09 » TREND MICRO
  - 10 » eEYE
  - 11 » MARKMONITOR
  - 12 » SKYBOX
  - 13 » 3VR
  - 14 » AIRMAGNET
  - 15 » PGP
  - 16 » SECURED EMAIL
  - 17 » REDSEAL
  - 18 » BIGFIX
  - 19 » 41ST PARAMETER
  - 20 » SECUWARE
  - 21 » nCIRCLE
  - 22 » ARCSIGHT
  - 23 » AXS-ONE
  - 24 » INCARD TECHNOLOGIES
  - 25 » MESSAGELABS



13200 Metcalf, Suite 300  
Overland Park, KS 66213  
Main: 913-851-9137  
Fax: 913-239-1888