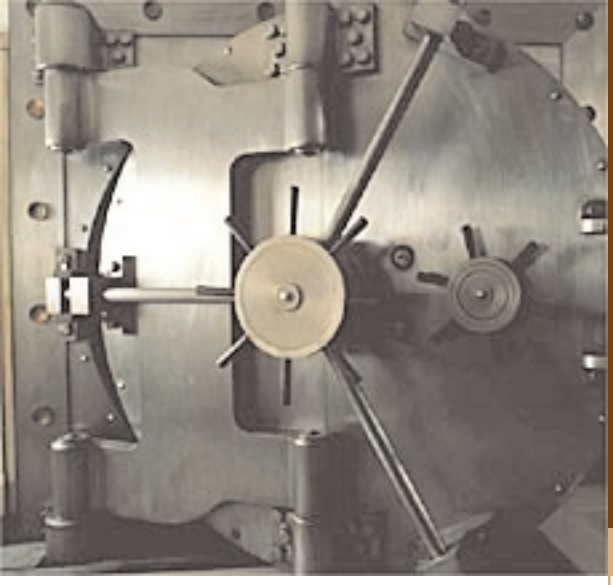


PRICEWATERHOUSECOOPERS

# The Secure Solution

*A monthly newsletter brought to you by the Security & Privacy Practice of PricewaterhouseCoopers*

VOLUME 19, OCTOBER 2003

## *In This Issue:*

This edition of *The Secure Solution*, a monthly newsletter from the Security & Privacy Practice of PricewaterhouseCoopers, includes the following: a new vulnerability scanning and analysis service; a thought leadership article on Identity Theft; a Threat & Vulnerability case study; plus upcoming events covering worldwide security issues.

Each month, we will produce a newsletter providing timely, topical information about security issues. If you should have any questions about our newsletter or our Security & Privacy Practice, please contact one of our marketing professionals listed below.

### Who To Contact:

**James F. Kelly**
Americas Marketing Leader
Global Risk Management Solutions
PricewaterhouseCoopers
415.498.5376
james.f.kelly@us.pwc.com

**Kate Oliver**
Marketing Director
Security and Privacy Practice
PricewaterhouseCoopers
860.241.7333
kathryn.oliver@us.pwc.com

## Introducing BoundaryPatrol™ — The Vulnerability Scanning and Analysis Service from PricewaterhouseCoopers

Is your Web environment vulnerable to threats and attacks? For example, is your company undergoing a major change such as implementing a significant external facing application? Are you currently deploying a Web-based system? Adding a portal? Upgrading your network infrastructure and/or operating system? Experiencing high turnover? Using a decentralised IT model? In the midst of a major merger?

If your answer to any of these questions is "yes," then you may need PricewaterhouseCoopers' BoundaryPatrol™ — an independent assessment of the vulnerabilities associated with your Internet-facing environment. Rather than scanning your systems from different business units with various scanning technologies, the BoundaryPatrol service performs vulnerability scanning using the latest vulnerability signatures, automated false-positive reduction techniques and leading security practices.

"This new service offers a standardised approach to identifying security vulnerabilities across an organisation's Internet connections," says Fred Rica, Partner, PricewaterhouseCoopers' Security and Privacy practice. "Overall, it positively identifies security vulnerabilities and root causes, significantly reduces false-positives and the trending of vulnerabilities – all at an economical price. As a subscription-based PwC service, BoundaryPatrol enables companies to schedule vulnerability scanning at regular intervals, while leveraging PwC's security experience and best practices."

### A Cost-Effective Approach to Vulnerability Scanning and Analysis

The BoundaryPatrol service is cost-effective and flexible, providing you with the security experience and business knowledge needed to strengthen your Internet-facing security posture. It frees up limited security resources to manage more strategic security initiatives while enabling you to proactively identify, track and correct vulnerabilities before a security incident occurs.

One of the key elements of effective Vulnerability Management is the development of vulnerability scanning capabilities that focus on an organisation's critical information assets that have the greatest security risk. "Our service offers a proven technology solution," adds Rica, "based on field tested methodologies, lab testing and successful client deployments coupled with PwC's understanding of business risk and industry issues. This service allows a business to leverage our research of security vulnerabilities, our understanding of global IT operations and our ability to deliver budget-friendly vulnerability scanning to an enterprise."

### What BoundaryPatrol Offers Your Company

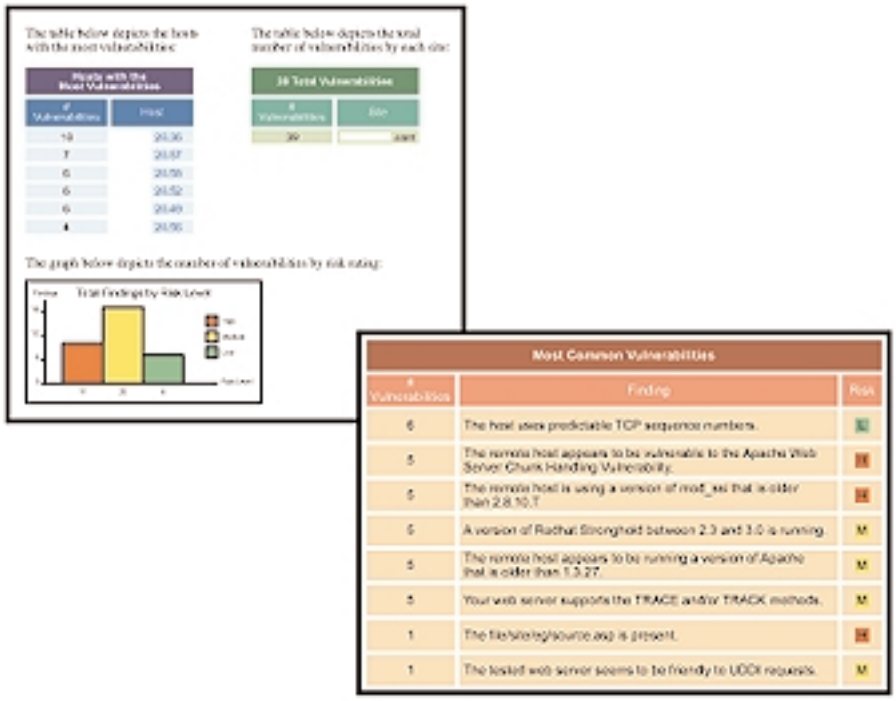
This service provides companies with a comprehensive vulnerability scanning solution that:

- **Is a simple, affordable subscription service**, tailored to meet your

(see next page)

*This service provides an independent, expert analysis of the security vulnerabilities associated with your Internet-facing environment. Rather than scanning your systems from different business units with various scanning technologies, the BoundaryPatrol service performs vulnerability scanning using the latest vulnerability signatures, automated false-positive reduction techniques and leading security practices.*

organisation's vulnerability scanning requirements;
- Lets you choose where to scan and determines how often — usually quarterly — **without the cost burden of an annual license fee**;
- **Determines the schedule of when vulnerability scanning can occur**, taking into consideration blackout windows and ISP notification;
- **Offers a comprehensive Internet Footprint and root cause analysis**, proactively identifying gaps and deficiencies of Internet-facing systems;
- **Makes recommendations for corrective actions** based on industry-leading practices;
- **Provides detailed explanations** of the security implications and risks of the exposures found related to each security analysis;
- **Supplies trending summaries** using the initial scan results as a baseline;
- **Takes advantage of PricewaterhouseCoopers' extensive security experience** and industry leadership with corporate internal control and regulatory compliance issues; and
- **Ensures your company's environment is consistently monitored** to identify problems and continue to improve security.




*BoundaryPatrol's Report Examples*

## How BoundaryPatrol Works

"When we perform a BoundaryPatrol scan," says Rica, "we determine the global baseline Internet Footprint of an organization, active vulnerabilities, risk levels, levels of effort to remediate these vulnerabilities and recommended corrective actions. In addition, we identify key themes or trends in the scanning results that are the root causes of these vulnerabilities. The scan will identify vulnerabilities that can be exploited either by viruses — for example, being attacked by the Blaster worm — or by an Internet hacker. The reports highlight susceptibility to an issue and provide you the information you need to prevent a problem before it happens."

How frequently BoundaryPatrol works depends on the number of systems a company has facing the Internet and how often a scan is scheduled. At the practical and tactical level, the scan identifies a company's susceptibility to a security breach and the root causes of that susceptibility. In many cases, companies simply don't have effective security policies and standards in place.


(see next page)

*"Many of our clients choose to run quarterly scans… When performing regular scans, you can clearly see security vulnerability trends and make solid management-level recommendations. Over time, we can see tangible results as the client focuses security resources on remediating identified vulnerabilities and as they focus on areas that need continued attention."*

*— Fred Rica, Partner, PricewaterhouseCoopers*

"Many of our clients choose to run quarterly scans," adds Rica. "When performing regular scans, you can clearly see security vulnerability trends and make solid management-level recommendations. Over time, we can see tangible results as the client focuses security resources on remediating identified vulnerabilities and as they focus on areas that need continued attention. "

Furthermore, he says, "We believe vulnerability scanning is a fundamental capability that every organisation needs to address. The fact is, traditional approaches to vulnerability scanning have been addressed solely from a technology perspective. This approach has yielded limited value to the business that a security organization is tasked with supporting."

"The BoundaryPatrol service addresses vulnerability scanning from a people, process and technology perspective, helping companies understand that security is much more than technology. And the service is offered at a cost-effective price point, positioning it as a great value for any organization," concludes Rica.

**See what we did for an insurance company.**

### Download Our Brochure

To learn more about how the BoundaryPatrol™ service from PricewaterhouseCoopers can help your company cost-effectively manage technology vulnerabilities, download our brochure now.

Or contact Fred Rica, Partner, PricewaterhouseCoopers, 973-236-4052.

## Identity Theft and How to Prevent It: *Reporting* on Request

*The editors of "The Secure Solution" often receive requests from readers about topical storylines. This is the first in our series of articles prompted by suggestions from our audience.*

Ask Gail Simon or Kathy Bentley (not their real names) how much pain, angst and anguish they suffered when someone stole their identities in mid-2003.

Try to realise that it took them both the better part of a month to meet with the local police, to sift through the labyrinth of new accounts created by others in their names, to rectify bank statements, and to clear their credit ratings.

Then hope it never happens to you.

Both of these women were victims of two Northern California theft rings with similar methodologies. Computer merchandise was bought online with the victims' credit cards or in their names and was shipped to their home addresses. "These thieves usually had someone waiting for the delivery truck at our front door," says Ms. Simon. "They met the driver, then simply drove the merchandise away. One day, I was lucky they missed the truck and the box was picked up by my mother."

### A Global Epidemic of Stolen Identities

The global identity theft epidemic is a very painful, sometimes expensive, and always frustrating experience for its victims.

Gartner defines identity theft as the theft of personal information (such as a Social

(see next page)

### One Victim's Story: How One Delivery Triggered Her Investigation

Consider the tale of woe of Ms. Simon, a San Francisco-based fundraising professional. She first realised her identity had been stolen when a new computer monitor was shipped to her mother's home.

"Mom called to thank me for the gift," says Ms. Simon. "But I told her I hadn't ordered anything! We discovered the last four digits of the credit card used didn't match any of ours. The San Francisco Police Department and the FBI told us our identities had been stolen. I determined that someone had set up four new credit cards in false names using my account and one using Mom's at another bank — all with my address — and possibly with a new driver's license with their picture and my driver's license number."

The damage over six weeks wasn't isolated to their credit card accounts. "These thieves were very sophisticated," she continues. "When we went online to check the balances on our bank accounts, we noticed counterfeit checks had already been written on both my Mom's account and mine, completely wiping one account out. Luckily, our bank reimbursed us for about $5,000 in charged goods and counterfeit checks within two weeks. But we still don't know how the thieves got the bank account numbers because we shred every bank statement, credit card statement, plus our receipts."

On Ms. Simon's checking and credit card accounts:

- It took her a week of full time investigation to discover the new accounts that had been set up in her name at other local banks;
- The charged merchandise was shipped to four different San Francisco addresses;
- There were two names on her new checking account: one was hers and one was the thief's — probably another stolen identity; and
- Her new bank account's balance was spread via electronic transfer to about 10 different accounts.

"I surmise it was an inside job at the bank," says Ms. Simon. "Unfortunately, I don't know if the FBI ever caught these thieves. Because we were innocent of these purchases, we did not have to pay for the items that were bought through our bank account."

The last thing Ms. Simon did was to call the three major credit bureau companies. "I put a security freeze, not an alert, on my name and Social Security number with the credit bureaus. I recommend everyone should get a credit report every three months to ensure your information is still correct and to discover possible illegal activity."

Security, driver's license or passport number) and use of the data to secure a loan or for some other illegal end. [1]

According to Right on the Money, April 30, 2003, "it takes the average consumer a full year to realize their identity has been stolen. Once they find out, that's when the clock really starts ticking – the average victim will spend 175 hours of their own personal time cleaning up the financial mess left behind."

The extent of this crime is far worse than you may have heard. A recent Federal Trade Commission survey notes:

- There were **9.9 million victims of Identity Theft** in the US during 2002; [2]
- **Nearly 1 in 8 adults** — 27.3 million Americans — have had their **credit card or identity borrowed**, or their credit rating ruined, over the past five years; [2]
- Overall, this type of crime cost **US businesses and consumers $48 billion** in 2002, with consumers losing about $5 billion; [2]
- **Over 3.2 million consumers discovered that new charge accounts** were opened and other frauds had been committed in their name; [1]
- **6.5 million victims reported misuse** of their credit card accounts; [1]
- Globally, people in the **United Kingdom, Japan and Canada** are also being victimized; [3]

Fortunately, there's a ray of sunshine. A Spring 2003 FTC survey of 4,000 people discovered that new incidents of identity theft — after nearly doubling for two to three years — are now growing more slowly and tend to involve less money. [2]

"Banks are wising up to the problem, says Howard Beales, director of the FTC's consumer-protection division, "making it more difficult for scam artists to set up fraudulent credit cards, and consumers are spotting suspicious activity on their accounts earlier." [2]

## How to Protect Your Identity: Tips for Consumers and Credit Card Issuers

According to "Reduce Identity Theft by Rectifying Too-Easy Credit Issuance," a September 4, 2003 Market Analysis by Avivah Litan at Gartner, to alleviate identity theft fraud, the FTC recommends educating consumers to be more careful in disseminating credit information.

"Gartner's approach focuses on the source of illegal credit — credit card issuers, cell phone service providers, banks, retailers and businesses that extend credit," says Litan. "Such actions will likely ease the pain and ramifications of identity theft by making it harder for thieves to get credit. But of course, it won't prevent thieves from stealing identity information for other ends." [1]

## The US Postal Service Offers More Help

At the United States Postal Service Website, these Identity Theft tips are provided:

- Review your consumer credit reports annually;
- Shred and destroy unwanted documents that contain personal information;
- Deposit mail in U.S. Postal Service collection boxes;
- Don't leave mail in your mailbox overnight or on weekends. [4]

Additionally, Mark Lobel, Senior Manager, Security and Privacy Services, PricewaterhouseCoopers recommends that you should review your bank and credit card accounts online quarterly for suspicious activity, and report any non-authorised costs to your bank or retail companies within 60 days so that you're not liable for the purchases.

"Consumers are learning to look for signs of trouble," says Howard Beales, the FTC's

(see next page)

### A Second Victim's Story: $30,000 in Fraudulent Chargers

"Someone got my credit card number and used the account," says Kathy Bentley, a sales executive in Concord, California. "The thief charged about $30,000 worth of computer and digital equipment from online stores."

With a law enforcement background, she investigated. "I called the police, cancelled my account, and called the online companies to find out when the goods were ordered. I was told the buyer authorized the delivery company to drop off the merchandise without a signature to my home. Someone was intercepting the goods from my front door."

She asked her bank to send her a new credit card. But by the time she received it, the new account had already been used to buy more online computer goods. That happened twice more with two new cards.

"It was a bit scary. Someone knew my name, address, date of birth, mother's maiden name — all facts known only by my bank. So I called the three major credit companies and put a hold alert on my credit. Then, because I still had my credit card that was being used by others, my bank asked me to file a fraud report. They made the thousands of dollars in charges disappear. But even though I filed the report and was not liable, the police couldn't prevent this from happening."

In hindsight, she offers these words of advice: "A shredder is your first line of defense. Second, be aware of what's happening with your credit cards. Third, don't assume because you put a credit watch on your Social Security Number that it's safe. And continue to make periodic reviews of your credit report."

consumer-protection division director, noting that one-third of victims surveyed said they noticed suspicious activity within a week. "Education, outreach and media reports are helping consumers to wise up." [2]

### For More Information

Contact Mark Lobel, Senior Manager, PricewaterhouseCoopers, 646-471-5731.

Sources:

[1] "Reduce Identity Theft by Rectifying Too-Easy Credit Issuance", Gartner, Market Analysis, Avivah Litan, September 4, 2003

[2] "Identity Theft Strikes 1 in 8 Adults, FTC Says", Technology – Reuters, Andy Sullivan, September 3, 2003,

[3] "CR Investigates: Stop Thieves from Stealing You", Consumer Reports, October 2003

[4] United States Postal Service Website: http://www.usps.com/postalinspectors/idthft_ncpw.htm

## Threat & Vulnerability Case Study: What We're Doing For a Major Insurance Company

### Description of Client's Business

The client is a major insurance company based in the US, with a large global network of Websites and other systems across three continents.

### The Client's Challenge

"This organisation was challenged with how to protect its global network and Internet-facing systems from increased attacks and threats," says Fred Rica, Partner, Security & Privacy Practice, PricewaterhouseCoopers. "It was also reacting to the changing regulatory landscape with security and privacy regulations evolving from such varied organisations as the US Federal Government, insurance industry governing bodies, and the overall European Union."

The rules and regulations vary in their scope and level of specificity, but the overall trend in the rules directs the holder or processor of protected information to exercise security mechanisms to protect and monitor this information, both in transit and at rest. The penalties for failure to comply vary depending on the country and the regulation, but can include monetary fines or even criminal prosecution.

The corporation's IT organisation was decentralised geographically, with only a small security organisation to cover hundreds of systems and network segments. Its security organisation:

- Was struggling with tracking how many sites and which sites were connected to the Internet at any given time;
- Had no way to determine if their systems were vulnerable to attacks; and
- Spent most of its time with security remediation.

### The PricewaterhouseCoopers Solution

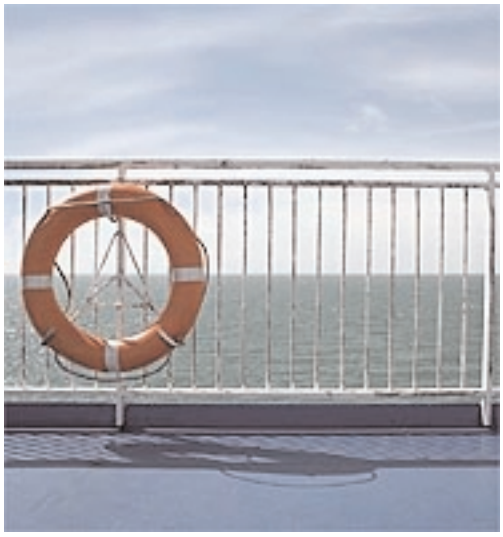
"The insurance company engaged PricewaterhouseCoopers' BoundaryPatrol™ Vulnerability Scanning and Analysis service to augment its existing security team and ensure that their Internet-facing systems were covered," adds Rica.

PwC's security consultants:

- Began by conducting research to confirm and verify their IP network range;
- Established the baseline, or Internet footprint analysis, for the corporation to begin the vulnerability scanning and detection process;



(see next page)



*"The insurance company engaged PricewaterhouseCoopers' BoundaryPatrol™ Vulnerability Scanning and Analysis service to augment its existing security team and ensure that their Internet-facing systems were covered."*

*– Fred Rica, Partner, PricewaterhouseCoopers*

- Conducted a series of four quarterly scans from PwC's Vulnerability Lab;
- Identified the weaknesses in the network perimeter through the scans, which included the entire external-facing network;
- Produced a list of issues with each scan that they could then prioritise and delegate to the various IT and business groups to fix.

PwC worked with the IT and security organisations to customise their vulnerability report deliverables. After each scan, the corporation's security team was provided with a report package, broken down by country, detailing the vulnerabilities that were detected. Each report contained a diagram that showed the top 10 issues for that scan which was beneficial to the security team to help them quickly identify where to focus their limited resources.

The Vulnerability Analysis reports are now distributed to each country's IT department and are used to track the correction of vulnerabilities, the creation of new sites and the patch management status of existing sites. Executive reports are part of the Vulnerability Scanning and Analysis report package and help senior management understand the most significant findings and recommendations.

### Benefits/Results to the Client

By conducting a series of scans over a one-year period, the corporation was able to see the trends for the detected vulnerabilities across their entire enterprise. The IT and Security organisation:

- Focused its time and resources on solving problems based on their priorities and business requirements;
- Could see that the number of issues found — each time a scan was performed —was reduced and its security posture was improved;
- Is finally back in control over its Internet environment; and
- Can continue to grow its Web presence with the confidence that the proper security controls are now in place.

### For More Information

To learn more about how the BoundaryPatrol™ service from PricewaterhouseCoopers can help your company cost-effectively manage technology vulnerabilities, contact Fred Rica, Partner, PricewaterhouseCoopers, 973-236-4052.

## Mark Your Calendars! Upcoming Conferences, Seminars and Webinars

Join PricewaterhouseCoopers and our Alliance Vendors at these important upcoming security conferences and events.

### SECURITY CONFERENCES

Executive Dialogue on Identity Management — Led by Earl Perkins of META Group

| | |
|---|---|
| Sponsored by: | PricewaterhouseCoopers LLP, Microsoft, Oblix and OpenNetwork |
| Date: | November 6, 2003 |
| Location: | Westin Hotel, 70 Third Avenue, Waltham, MA, 8:00 – 10:30 A.M. |

(See next page)

*Don't miss these important security events.*

Explore the business value and the challenges of deploying identity management solutions in major companies. Gain insight into how large organisations are leveraging their platform investments, phasing implementation of identity management and implementing in a web services environment. This is an opportunity to learn about best practices, engage industry experts in a question and answer format and gauge your security posture and plans against those of your peers.

Panelists include:
Sandeep Sinha, Lead Product Manager—Identity Management, Microsoft Corporation
Gerard Verweij, Partner, Security & Privacy Practice, PricewaterhouseCoopers
Representative from Oblix
Representative from OpenNetwork

Register online or call 1-877-MSEVENT (event code 1032238068).
For more information, please contact carol.j.zielinski@us.pwc.com, 312-298-3199.

### The Symantec SecureXchange User Conference

Sponsored by : Symantec
Date: November 4-7, 2003
Location: Sheraton Premiere Tysons Corner, Vienna, VA (near Washington, D.C.)

Security-conscious Systems Engineers, Network Administrators, and IT Managers will be gathering for this one-of-a-kind conference. Register today at no charge.

Register online.

### Sarbanes-Oxley Compliance for Customers of SAP Software

Sponsored by: Wellesley Information Services (WIS)
Date: November 3-5, 2003
Location: Marriott Crystal Gateway, Arlington, VA (Washington, D.C.)

This conference is the definitive place to learn precisely how to bring your organization into compliance with the Sarbanes-Oxley Act. Highlights include:

- 60 in-depth sessions
- 5 comprehensive tracks
- Keynote address by Congressman Michael Oxley
- Industry forums
- Pre-conference "Jumpstart" session
- Ask-the-expert meetings
- Case studies
- Plus, special events and networking opportunities

Register online at: http://www.socompliance.com/

## UPCOMING WEBCASTS

To be announced…

## ARCHIVED SARBANES-OXLEY WEBINARS

### Microsoft Executive Circle Presents: How does Identity Management Support Sarbanex-Oxley Compliance?

Presented by: Steve Wilkens, Director, PricewaterhouseCoopers LLP; Ashley Arbuckle, CISSP Manager, Security & Privacy Practice, PricewaterhouseCoopers LLP; and Sandeep Sinha, Lead Product Manager, Microsoft Corporation
This event was held live on August 13, 2003.
URL for viewing: www.microsoft.com/usa/webcasts/ondemand/2141.asp

(see next page)

*Join us at these upcoming industry events.*

**PricewaterhouseCoopers On Demand Webcasts**

**Rebroadcast of Two-part Webcast: "Sarbanes-Oxley: Leveraging Your SAP Environment to Enhance Financial Controls"**

Part One - March 20, 2003
Part Two - April 3, 2003
URL for viewing: www.pwc.com/extweb/ncevents.nsf/DocID/C9A3A9AA9241A2AB85256CE50062EB08

**ARCHIVED IDENTITY MANAGEMENT WEBINARS**

**The Power of Roles in Identity Management, Featuring Merrill Lynch – September 18, 2003**

Join PricewaterhouseCoopers, Netegrity and special guest Merrill Lynch for a practical discussion on role-based Identity and Access Management. We'll share best practices, strategies, and a client example presented by Dean Mazboudi, Vice President — Data & Technology Architecture from Merrill Lynch.
URL for viewing: http://members.netegrity.com/Event.cfm?Id=473&campaction=60

**Microsoft Executive Circle Presents: Identity Management in the HealthCare Industry – July 22, 2003**

URL for viewing: www.microsoft.com/usa/webcasts/ondemand/2089.asp

**Microsoft Executive Circle Presents: Planning for Identity and Access Management Solution – June 17, 2003**

URL for viewing: www.microsoft.com/usa/webcasts/ondemand/1987.asp

**Netegrity On Demand Webcasts**

**Best Practices for Migrating from SiteMinder v4.x to v5.5 - July 31, 2003**

URL for viewing: www.netegrity.com/events/events.cfm?page=eventsarchived

**Real-World Identity and Access Management Deployment Experiences - An Interactive Panel Discussion - June 19, 2003**

URL for viewing: www.netegrity.com/events/events.cfm?page=eventsarchived

**WANT TO KNOW MORE?**

Please contact Bryan Welch, 415.498.7991.