

The Secure Solution

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

VOLUME 14, MARCH 2003

In This Issue:

This edition of *The Secure Solution*, a monthly newsletter from the Security & Privacy Practice of PricewaterhouseCoopers, includes the following: the Operate stage of our proprietary Enterprise Business Security Model™, a look behind the scenes at how PwC counts the annual Oscar® votes, a White Paper about The Value of Identity Management for the Communications Industry, a case study for a major US financial client, 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.pwcglobal.com

Kate Oliver

Marketing Director
Security and Privacy Practice
PricewaterhouseCoopers
860.241.7333
kathryn.oliver@us.pwcglobal.com

The Third Critical Step In A Comprehensive Approach to Security: The OPERATE Stage of the Enterprise Security Business Model™

This article is the fourth in a six-part series covering the ESBM™ and PricewaterhouseCoopers' vision of how security delivers value across the enterprise.

As the Global Leader of PricewaterhouseCoopers' Security & Privacy practice, Joe Duffy heads up one of the world's largest security services practices. Overseeing at least 400 security professionals in the U.S. and another 1,200 around the globe, he's a frequent media commentator on security issues. Few experts are in a better position to understand information security today.

"Our clients are leveraging the Internet," he begins, "in order to drive incredible value and benefits right to the bottom line. By connecting seamlessly with customers, suppliers, business partners, and employees around the world, they are able to drive down costs, and increase efficiency, and...in many cases...drive revenue opportunities."

"But to leverage the Internet, " he adds, "you have to think about security and privacy. You have to balance two seemingly opposite capabilities: letting the right people in to get access to the information and the transactions they need to do business...while also keeping the wrong people out."

As any security professional will tell you, it's not easy.

Security Today: Protection and Enablement

The concepts of inclusion and exclusion that Duffy is getting at lie at the heart of PricewaterhouseCoopers' vision of how security adds value to an enterprise. The Security of Inclusion represents the business imperative that the right people — including your customers, suppliers, partners, and the enterprise workforce — require controlled access to the right resources. At the same time, the Security of Exclusion represents the business imperative that an organization's information assets must be protected to ensure integrity, privacy, and reliability.

Companies Have Different Internal "Buyers" of Security

Duffy continues, "What our clients are struggling with, however, is that striking the right balance between inclusion and exclusion can be a difficult proposition." Companies typically have different internal security constituents — internal "buyers" of security — who are looking for different security payoffs. For example, on the one hand, their sales people tend to push for Security of Inclusion solutions — features that increase customer satisfaction and allow them to reach into the enterprise. On the other hand, their IT people tend to gravitate towards Security of Exclusion capabilities that will protect the integrity of their critical business assets.



To leverage the Internet, you have to... balance two seemingly opposite capabilities: letting the right people in to get access to the information... they need to do business...while also keeping the wrong people out."

Joe Duffy, Global Leader, Security & Privacy Practice, PricewaterhouseCoopers

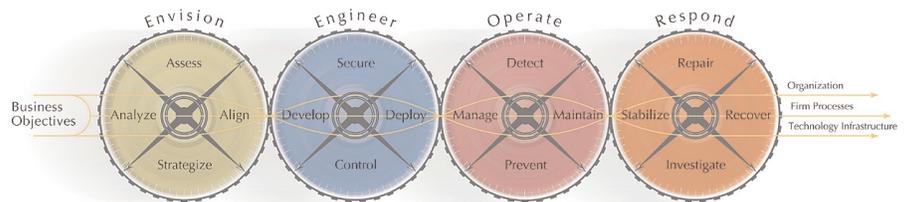
And that's the point: getting both your IT people and your business people to agree is just the beginning. The real difficulty is in finding a working framework to guide decision-making.

Which is why the Enterprise Security Business Model™ is so important.

The Enterprise Security Business Model

As discussed in prior articles, the ESBM™ is the first comprehensive security model that illustrates how to identify, create, capture, and sustain the value of security in an organization by managing the inherent trade-offs between enablement and protection of an enterprise's most valuable resource – its information assets.

The model is comprised of four primary activities – Envision, Engineer, Operate, and Respond – activities that are enacted in alignment with an organization's business objectives and its support capabilities in order to generate security value. Articles on the ENVISION stage and on the ENGINEER stage have been published in prior months. This article focuses on the OPERATE stage.



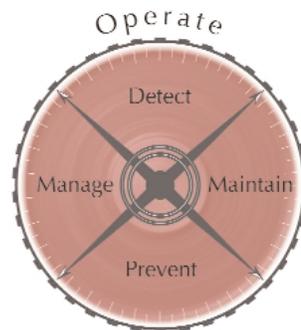
PricewaterhouseCoopers' Enterprise Security Business Model™

Why the OPERATE Stage Plays A Critical Role

Michael Van Demark and Todd Feinman join the interview. They're Senior Managers in the Security & Privacy Practice at PricewaterhouseCoopers – and, backed by the firm's decades of experience in IT security – they were a part of the team that developed the ESBM.

"What makes the OPERATE stage so crucial", explains Van Demark "is that this is precisely where the value of security for an enterprise is actually captured. Or not, as is often the case."

The OPERATE stage is defined as the continuous management of the security and controls built within the enterprise across the infrastructure of all your technologies and processes. This activity includes updating, enhancing, and monitoring the technology environment, as well as staying current with known threats. Its purpose is to continuously manage a secure environment, monitor for anomalous events, implement appropriate mitigating controls, integrate with the core IT environment and escalate appropriately if events become incidents or emergencies.



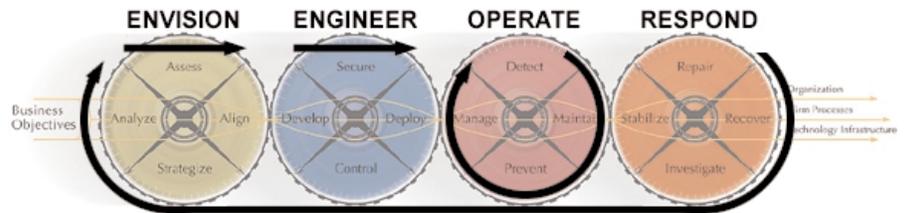
The Operate stage of the Enterprise Security Business Model™ from PricewaterhouseCoopers

Feinman is speaking. "Typically, by the time we are brought in", he says, "the client is deep into Operate...and having difficulties. But unless the organization has (see next page)

The OPERATE stage's key dependence on Envision, and Engineer, is all the more important because, as the figure below illustrates, OPERATE is the only stage which continues to function on a 24/7 basis, 365 days a year.

Envisioned correctly, and Engineered appropriately, the tasks it undertakes in the Operate phase — however well-carried out — may not in fact contribute value to their enterprise...may not support their business objectives – or may not be efficiently aligned with their security resources — their people, their processes, and their technology infrastructure”.

The OPERATE stage's key dependence on Envision, and Engineer, is all the more important because, as this figure illustrates, OPERATE is the only stage which continues to function on a 24/7 basis, 365 days a year.



While the primary activities in Envision and Engineer occur sequentially, those in Operate are cyclical, and those in Respond are undertaken on an as-needed basis.

A customized, top-down approach for each client's environment

Duffy has been listening for the last few minutes. He wants to be sure that we get this right. "It's important to have technology..." he explains, "...but it's also important to understand where technology fits in an overall architecture. We believe that it is important to approach this from the top down in a way that takes into account the technology, process, and organizational issues unique to each of our client's operating environments."

Duffy stops to take a call from one of his global colleagues. Information has always been shared across this worldwide practice, but today, with the ESBM platform in place, the practice has a common language, approach, and methodology for helping clients build a secure infrastructure.

That's a pretty unique position to be in, even in this industry. It means that multinational organizations can expect PricewaterhouseCoopers to deliver common methodologies across borders; and can expect PwC security professionals in Germany to speak the same "language" as those based in Japan. That's part of what Joe Duffy means when he says his practice delivers "world class security solutions."

One thing is clear. Even if Duffy and PricewaterhouseCoopers can't tell you what the future will hold, they can help you with the security infrastructure necessary to prepare for it.

To find out more...

For more information about the Enterprise Security Business Model — please contact Michael Van Demark, 646.471.8859, or Todd Feinman, 646.471.7299.

© 2003, PricewaterhouseCoopers LLP. All rights reserved. "ESBM" and "Enterprise Security Business Model" are service marks of PricewaterhouseCoopers.



“Observing the ceremonies and working backstage is a whole different adventure.”

– Greg Garrison & Rick Rosas, Ballot Partners, PricewaterhouseCoopers

A Month in the Life of a Ballot

The ballots for nominations were mailed to the 5,800 members of the Academy on January 10th. They had a few weeks to return their nominations, before they were announced to the world on February 11th.

Every member, except for Associate and Retired members, may vote for Best Picture, but for the other categories the members may only select nominees in the respective branch of the Academy to which they belong — directors nominate directors, cinematographers nominate cinematographers, and so on.

The nominations themselves are determined by a so-called preferential system, meaning that each voting Academy member votes for films and individual achievements in order of their preference. The final tabulations are made by the plurality system, so the nominee with the most votes in a particular category wins.

“And The Oscar® Goes To”... How PwC Counts The Ballots

As an estimated 800 million people worldwide watched the 75th Annual Academy Awards® Presentation from Hollywood on Sunday, March 23, the most nervous pair of people on stage wasn't host Steve Martin and four-time winner Jack Nicholson.

It wasn't “Chicago” stars, Catherine Zeta-Jones and Renée Zellweger. It wasn't even Best Supporting Actor nominees, Paul Newman and Christopher Walken. Nor was it any other pair of multi-talented stars of the big screen.

Actually, it was Greg Garrison and Rick Rosas, PricewaterhouseCoopers' Ballot Partners, who stood in the wings of the Los Angeles Shrine Auditorium and once again handed the envelopes to the Award presenters. This marked the 69th year in PwC's heralded partnership with the Academy of Motion Picture Arts & Sciences, anchoring the firm's global entertainment practice.

The Most Glamorous Jobs in Accounting

Either Greg or Rick would probably tell you that they have the most glamorous and exciting jobs in accounting. However, as Greg will also tell you, “observing the ceremonies and working backstage is a whole different adventure.”

Greg Garrison heads PricewaterhouseCoopers' Assurance and Business Advisory Services Practice. During more than 27 years with the firm, he's led the Entertainment and Media practice, and provided accounting and business advisory services to large multinational clients in the entertainment and consumer products industries. Greg has been the lead partner serving the Academy of Motion Picture Arts and Sciences since 1995.

In 2002, Rick Rosas, a partner in PricewaterhouseCoopers' Entertainment and Media Practice, was named the new co-ballot partner. He's practised for more than 15 years, and since he joined the firm in 1996 has provided tax services to the Academy as well as leading entertainment companies.

Counting the Ballots And Maintaining Secrecy

PricewaterhouseCoopers approaches this particular annual engagement with these goals: accurately counting the ballots, while maintaining the legendary secrecy and integrity that has always surrounded the voting process.

In fact, PricewaterhouseCoopers is so secretive about the entire balloting and tabulation process that Bob Hope once joked that to insure the secrecy of the results, the firm “shoots the secretaries.” Happily, PricewaterhouseCoopers does nothing of the sort. But it is true that the names of Academy Award winners are probably the most closely guarded secrets in Hollywood — even the Academy's Governors have no idea who is going to win until the sealed envelopes are opened. The Academy Awards have been called “the most honest elections anywhere in the world.”

Locking In The Tabulators For Three Days

The ballots for the Awards' 24 categories are tabulated at a secret location known only to the members of the small PwC ballot team. The room in which the votes are tallied is locked at all times and only team members are ever allowed in. At the end of each of the hard days of counting, all the ballots and tabulation materials are locked in a safe, along with all tallies and related notes.

And, if that weren't enough, the final tally of the biggest awards is delayed until a day or two before the show. That way, the two partners managing the balloting — Greg Garrison and Rick Rosas — know the results for as short a time as possible. As an added precaution, Greg and Rick also memorize the results, then quiz each other to make sure they've remembered every name and every award. After all, they're the

“The actual ballot counting is clearly important to the show, but how we complete that role... reflects a number of the firm’s core values, including professionalism, integrity, confidentiality and accuracy.”

Here’s What Counts

The Academy’s trusted balloting partner has tallied some other interesting numbers that illustrate what has gone into ensuring that the town’s biggest secret is kept under wraps, and that the world’s most famous statuettes get into the hands of the right nominees.

415,000	The approximate number of ballots counted by PricewaterhouseCoopers in 69 years on the job.
2,400+	The number of winners’ envelopes stuffed since the envelope system was introduced in 1941.
1,700	The approximate number of “person-hours” it takes the PricewaterhouseCoopers team every year to count and verify the ballots by hand.
69	The number of years PricewaterhouseCoopers has conducted the Oscar® balloting.
50	The number of broadcasts PricewaterhouseCoopers partners have appeared on since 1953 – the year the Oscars® were first televised. The partners used to come on stage to hand-deliver the envelopes ; hence, “and the envelope please”, but this is now done just offstage.
7	The number of days it takes to count the ballots for nominations.
3	The number of days it takes to count the final ballots.
2	The number of firms who have conducted the ballot counting for the Academy Awards: Price Waterhouse and PricewaterhouseCoopers.

only people in the world who know who all of the winners are.

Armed Bodyguards And Other Security Precautions

To preserve the secrecy even longer, the final envelopes aren’t stuffed until the day of the Awards. Lined, opaque envelopes sealed with red wax were introduced in 1941, although today red stickers replace the wax. In fact, two sets of envelopes are prepared and separately hand-carried by Greg and Rick to the Awards ceremony. Armed bodyguards drive them to the ceremony and stay with them until the final envelope has been handed out.

While these security measures might seem rather stringent for a non-military operation, they are really nothing more than an extension of PwC’s commitment to preserve our clients’ privacy. As Greg Garrison is quick to point out, “The actual ballot counting is clearly important to the show, but how we complete that role is also important because it reflects a number of the firm’s core values, including professionalism, integrity, confidentiality and accuracy.”

After all this – and a global audience of 800 million people – who says accounting isn’t glitzy?

For More Information...

Visit the PricewaterhouseCoopers The Oscars® site.

The Value of Identity Management for the Communications Industry

This article is based on a White Paper from PricewaterhouseCoopers

Few sectors have had to weather the tidal shifts that are reshaping the competitive markets of the communications industry. Global regulatory changes have altered the rules of business. The rush of developments in digital technology has blurred the distinction between the communications, computing and media sectors. And with one sweep, the Telecommunications Act of 1996 has sundered the market-shaping barriers to entry that constrained industry competition for decades.

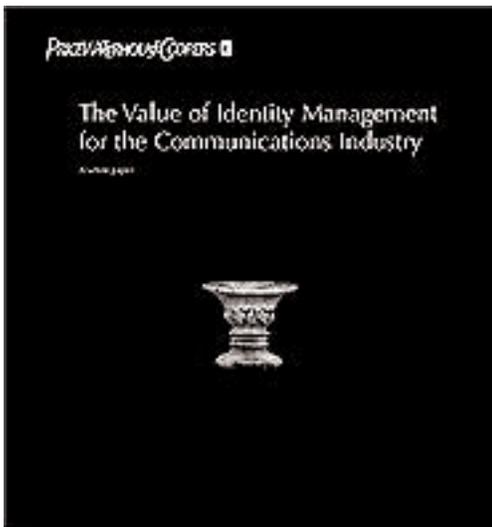
These singular events are among those that have resulted in a fundamental transformation of the communications landscape — one that has introduced new markets, new players, new challenges and — for those positioned to turn change to competitive advantage — new opportunities.

Objectives Require Critical Identity Management Capabilities

Senior executives in telecommunications companies understand that achieving their business objectives – not just in spite of the market turbulence, but precisely because of it – depends on having the right information technology infrastructure.

These leaders realize that:

- Privacy, security and accessibility to critical business and information assets enable all transactions, not just e-transactions;
- The ability to both protect and enable access to increasingly vast amounts of data — data that is frequently mission-critical and proprietary — is essential;
- The ability to effectively engage and transact business online directly with business partners, suppliers, customers and employees is now mandatory; and
- That when in balance, these two capabilities — enablement and protection — are fundamental to survival and profitability, especially given the treacherous crosscurrents in the communications industry.



With one sweep, the Telecommunications Act of 1996 has sundered the market-shaping barriers to entry that constrained industry competition for decades.

Building these capabilities requires, at the very least, a comprehensive Identity Management solution. One that helps improve cost efficiencies, enable access to resources and promote user satisfaction while providing a high degree of security. One that will also reduce the cost of managing user information, increase productivity for both users and administrators, and reduce the time-to-market for new initiatives.

Questions Communications Firms Are Asking

Though industry trends are increasing demand for centralized management of user identities, how to take the first steps, especially within the context of ongoing operations, existing infrastructure and uncertainties in market conditions, is not always clear.

Questions and concerns among senior IT professionals include the following:

- "How do I make sure the right people gain controlled access to resources? Once in, how do I get a single view of the user across the enterprise?"
- "How can I keep the wrong people out and manage my complex environment?"
- "How do I get ahead of the 'vulnerability curve'?"
- "In a world of limited time, money and resources, how do I begin to balance these two competing priorities – protection and enablement?"
- "How can I quickly respond when something bad happens?"
- "After an incident occurs, how do I 'stop the bleeding' and stabilize my organization?"

White Paper Scope and Approach

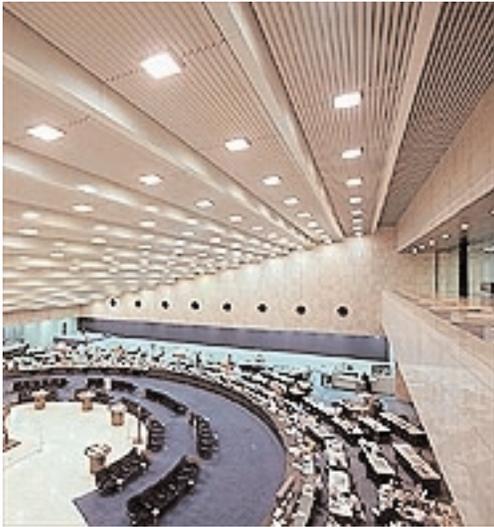
To read more about this topic, download our new White Paper on Identity Management for the Communications Industry. This White Paper addresses the industry trends in communications currently driving the demand for Identity Management, and articulates the primary benefits and technical components of a strategic Identity Management solution.

This report also presents market-leading research sponsored by PricewaterhouseCoopers and conducted by META Group on the key value metrics that drive Identity Management programs, including companies within the communications industry.

Finally, this document builds a case for approaching Identity Management within the comprehensive framework provided by the Enterprise Security Business Model™ in order to ensure that the benefits promised by Identity Management are delivered in full alignment with a company's business objectives and comprehensive security infrastructure.

To Find Out More...

Download the White Paper: The Value of Identity Management for the Communications Industry.



“Initially, a pilot program would enable 40,000 business customers, geared to roll-out to 100,000...”

Daniel Trieschmann, Senior Manager, Security & Privacy Practice, PricewaterhouseCoopers

Identity Management Case Study: What We Did For a Major US Financial Client

Description of Client’s Business

The client is one of the largest US-based financial institutions, with thousands of offices nationwide.

The Client’s Challenge

This company needed to address a competitive market need – business online banking. To kick-start the program, the CIO forged a strategic partnership with Microsoft using the Windows 2000 operating system, ASP.NET for building applications and XML Web services, as well as Microsoft’s Internet Security and Acceleration (ISA) Server 2000 firewall.

“Initially, a pilot program would enable 40,000 business customers, geared to roll-out to 100,000 at the end of the engagement. The end-game was that once BOB was successful, we could roll this out to millions of potential customers for consumer online banking,” says Dan Trieschmann, Senior Manager, Security & Privacy Practice, PricewaterhouseCoopers (PwC). The PwC project leader is Gary Loveland, Partner, Security & Privacy Practice.

The PricewaterhouseCoopers Solution

PricewaterhouseCoopers’ team was primarily engaged to help this client design and implement an Identity Management (IdM) infrastructure utilizing Oblix NetPoint 6.0 for their customer-facing Web and eBusiness initiatives. This robust IdM solution was intended to improve the end-user business customer experience, enhance security and simplify the administrative processes for them, ultimately reducing costs.

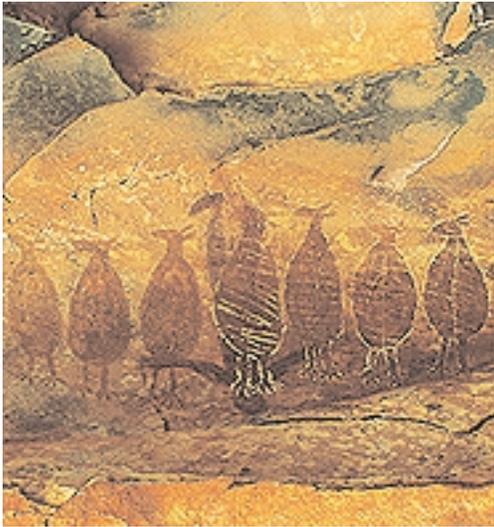
“We recognized that a Microsoft-centric site would enable the client to manage user profile information seamlessly through an integrated Identity Management solution,” adds Trieschmann. This solution enables the company to facilitate account set-up for business customers, access clients’ profile information, and allow back-end Contact Centers/Help Desk personnel to migrate user data.

By integrating Microsoft Active Directory for the user repository of 40,000 customers, PwC’s IdM access and identity management solution, deploying Oblix Netpoint 6.0:

- Allows business banking customers to transfer funds;
- Make payments online with bill paying modules;
- Schedule future payments;
- Delegate administration models;
- Print statements;
- View account histories;
- Stop payments;
- And more.

Currently, PwC is addressing the client’s needs with its global view of comprehensive enterprise security utilizing the Enterprise Security Business Model (ESBM)[™]. This four-stage process identifies, creates, captures and sustains the value of security in any organization. Through the framework of the ESBM, PwC is analyzing the company’s Public Key Infrastructure (PKI) process, business continuity, disaster recovery, incident response, patch management, and threat and vulnerability management.

PwC also reviewed the company’s internal controls policies for managing their PKI environment for digital signatures with a Microsoft internal certificate authority, then recommended improvements to existing controls.



Don't miss these important security events.

Benefits/Results to the Client

"The initial results have significantly exceeded the client's expectations," says Trieschmann. "With minimal advertising and promotion, our client expected 1,000 customers a month to sign-up for business online banking. They exceeded that in the first week."

The infrastructure and processes co-developed by the client, PricewaterhouseCoopers, Microsoft, and Oblix will also be leveraged to enhance the online banking capabilities for individual consumers.

In addition to assisting with the online banking initiative, PwC and Oblix have designed and implemented an Intranet identity infrastructure for the company's internal employees (50,000), enabling them with business-to-enterprise capabilities.

Contact Us

To find out more about PricewaterhouseCoopers' Identity Management solutions, please contact:
Daniel Trieschmann,
Senior Manager, Security & Privacy Practice
314.206.8781

Mark Your Calendars! Upcoming Conferences, Seminars and Webinars

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

SECURITY CONFERENCES

RSA Conference 2003

Sponsored by: RSA Security
Date: April 13-17, 2003
Location: Moscone Center, San Francisco
Register online at: <http://www.rsasecurity.com/conference/>

Be there for the world's leading e-security conference and expo. The annual RSA Conferences, the leading electronic/data security conferences worldwide, bring together IT professionals, developers, policy makers, industry leaders and academics to share information on technology, trends and best practices on diverse security topics such as identity theft, hacking, cyber-terrorism, biometrics, perimeter defense, secure web services, encryption and other related topics. Renowned for its rich content, these conferences are designed to educate security practitioners, business people and policy makers on the latest developments in technology and provide a forum for the exchange of ideas and networking with peers.

Gartner Enterprise IT Security Conference

Date: June 2-4, 2003
Location: Washington Hilton, Washington, D.C.
Register online at: <http://www.gartner.com/us/itsecurity>

This Summit brings together two powerful conferences in creating the definitive event for both private and public-sector IT security professionals. The exceptional scope of this event will provide a range of strategic insight and tactical direction to fully serve the concerns and priorities of IT security executives from Fortune 2000 enterprises, the federal government and the nation's critical-infrastructure entities.

Join us at these upcoming industry events.

BlackHat USA 2003 Briefings and Training

Sponsored by: Black Hat
Date: Training: July 28-29, 2003
Briefings: July 30-31, 2003
Location: Caesars Palace, Las Vegas
Register online at: <http://www.blackhat.com/>

SARBANES-OXLEY & CONTROLS WEBINARS

Two-Part Webcast: Sarbanes-Oxley: Leveraging Your SAP Environment to Enhance Financial Controls

Dates: Thursday, March 20
Thursday, April 3, 2003 at 2:00 pm (EST)/11:00 am (PST)

Presented by PricewaterhouseCoopers LLP & SAP

Attend from your desktop. This informative two-part Webcast series gives SAP customers and prospects guidance in complying with the Sarbanes-Oxley Act of 2002, including enhancement of internal control capabilities. Part Two will feature a comprehensive internal controls action plan.

Register online at: http://www.sap.com/mk/get/us_sarboxseries

IDENTITY MANAGEMENT WEBINARS

Webcast: Building a Secure Web Presence with Identity Management and SAML

Date: Thursday, April 3, 2003 at 11:00 am (EST)/8:00 am (PST)
Presented by: PricewaterhouseCoopers LLP and Oblix

Attend from your desktop. Join PricewaterhouseCoopers and Oblix for an interactive Web Seminar that addresses the challenges of keeping data secure while enabling user-friendly access. The Security Assertion Markup Language (SAML) is security standard for exchanging user authentication and authorization information. Our industry experts will discuss how to leverage Identity Management and SAML, to improve your constituents' online experience, gain competitive advantage, and leverage your security infrastructure while lowering operational costs.

Register online at: <http://webevents.broadcast.com/oblix/0403>

Webcast: Securely Managing Your Supply Chain with Identity and Access Management

Date: Tuesday, April 8, 2003 at 11:00 am (EDT)/8:00 am (PDT)
Presented by: PricewaterhouseCoopers LLP and Netegrity

Attend from your desktop. Learn how to build a secure Web presence with Identity and Access Management that will enable your supply chain, customers, employees and partners to access your manufacturing application data while enhancing security controls and reducing IT costs.

Register online at: <http://members.netegrity.com/Event.cfm?Id=412&campaction=60>

WANT TO KNOW MORE?

Please contact Bryan Welch, Global Risk Management Solutions, at bryan.r.welch@us.pwcglobal.com, 415.498.7991.