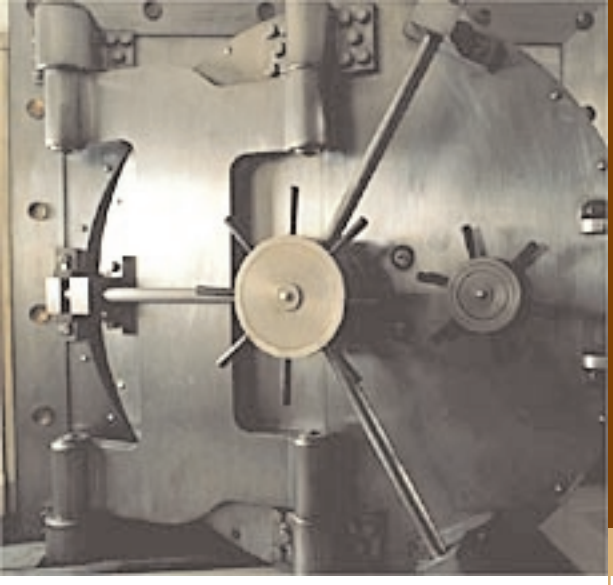


PRICEWATERHOUSECOOPERS

# The Secure Solution

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

VOLUME 20, NOVEMBER 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 risk management accelerator; a thought leadership article on HIPAA and security; a Vulnerability Detection case study; an overview of a comprehensive Information Security book; 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
Advisory
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 A New Risk Management Accelerator: Integrated Security Policy Management from PricewaterhouseCoopers

Until now, your organisation has most likely established Security Policies, had them authorised by management, created security standards for each platform, and published each of these documents on your global Intranet.

Or if you're a more sophisticated company, you've installed an enterprise security management compliance tool on your critical hosts, created specific policies to reflect your own security policy, and have scheduled automated compliance checks.

But with a dramatic increase in Internet security incidents, with concerns of compliance with new regulatory requirements, and with alignment of your IT infrastructure to corporate security policies, networks and operating systems, these best practices haven't been enough.

### Numerous Security Policy Management Issues to Overcome

Because today's organisation must perform these multiple tasks simultaneously, it's easy to get out of synch. The issues that are surfacing include:

- A lack of senior management understanding of security policy's level of compliance;
- No periodic reporting of security issues to senior management or to business stakeholders;
- A lack of adequate focus of resources on areas of non-compliance by security organisations;
- No historical view of compliance;
- Increased exposure to security threats;
- An inability to demonstrate compliance with government regulations in a timely manner;
- An inability to scale manual compliance processes to global organisations; and
- Overall, degradation of security posture due to increases in vulnerabilities.

### How our Integrated Security Policy Management Solution Can Help

The Integrated Security Policy Management (ISPM) Service from PricewaterhouseCoopers is designed to help organisations quickly and affordably align their IT infrastructure to comply with documented security policies. We work with your IT organisation to establish an integrated security policy management approach. We understand the information needs of each of the security stakeholders (e.g., Senior Management, IT and Security management) and can design solutions to satisfy each of their needs.

Next, we develop a prototype automated policy management solution that integrates compliance testing tools, extending existing IT operations processes and establishing



(see next page)

*"The bottom line is about bringing together your organisation, management processes, and technology to proactively manage vulnerabilities and reduce risk. This comprehensive service offering provides your organisation with sustainable processes and tools to ensure the confidentiality, integrity, and availability of information assets."*

*Joe Duffy, Partner and Global Leader, Security & Privacy Practice, PricewaterhouseCoopers*

a sustainable reporting process to client management. The reporting process determines a baseline compliance with corporate security policies and establishes targets and timeframes for achieving compliance.

Then, we design a technical solution to collect the raw security data, develop the processes to parse and disseminate the security status, and identify the resources required to sustain this program.

"The bottom line," adds Joe Duffy, Partner and Global Leader, PricewaterhouseCoopers' Security & Privacy Practice, "is about bringing together your organisation, management processes, and technology to proactively manage vulnerabilities and reduce risk. This comprehensive service offering provides your organisation with sustainable processes and tools to ensure the confidentiality, integrity, and availability of information assets."

### Benefits to Your Organisation

Designed to help you quickly assess and align your IT infrastructure to comply with your corporation's documented security policies, PwC's best-of-breed solutions and experienced security professionals work with your IT organisation to establish an integrated security policy management approach.

Benefits include:

- A **"Quick Start" approach** that minimises organisational impact and enables a client to show immediate results;
- **Benchmarking your IT controls** against our leading/best practice controls to analyse how to support your documented security policies;
- **The ability to quickly measure and report IT infrastructure compliance** against established security policies in a consistent manner across your enterprise;
- A documented, accepted **process to help ensure sustainability**;
- Process automation resulting in **increased efficiency**; and
- Processes that can be **leveraged across your enterprise**.

### Find Out More

To learn more about how the Integrated Security Policy Management service by PricewaterhouseCoopers can help your company cost-effectively manage compliance to your security policy, download our brochure.

Or contact Chris Miller, Partner, Security & Privacy Practice, PricewaterhouseCoopers, 678.419.1206.

## How HIPAA and Security Intersect: *Reporting on Request*

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

Exactly how secure or private is the health information for which your organisation is responsible?

In October, patients of a San Francisco Bay Area hospital realised that the security and privacy of their records was in jeopardy of being violated. A woman in Pakistan, where the data had been outsourced, had actually threatened to hold these patient records hostage, or worse, display them publicly, unless the hospital paid her more money.

"It's ironic," says Jeff Fusile, Partner-in-Charge, HIPAA Advisory Services, PricewaterhouseCoopers. "Choosing to outsource services whether inside or outside



(see next page)

*"HIPAA is about good security practices for all health care organisations. These regulations by the U.S. Department of Health & Human Services apply not only to most U.S. health care plans, providers and clearinghouses, but also to many employee-sponsored health and welfare plans. This expansion outside of strict health care entities makes the HIPAA security rule particularly impactful on the corporate community and presents a new risk in an already highly regulated environment."*

the country is often a decision made to save money - It appears in this instance that it may end up costing more. Regardless of how this specific issue is settled, it is becoming very clear that health care organisations (especially HIPAA covered entities) will need to apply a whole new level of rigor around the way in which they handle, safeguard and grant access to protected health information (PHI)."

"The real issue for all health care entities," adds Fusile, "is this: what processes will your organisation put in place to help ensure that you have a well protected environment, as well as reputable and reliable vendors? And what measures will be kept in place to ensure that it stays that way? Also, since privacy and security are interwoven, a discussion about one here encompasses the other."

## A Brief HIPAA History

According to the U.S. Department of Labor, the **Health Insurance Portability and Accountability Act (HIPAA)**, signed into law on August 21, 1996, offers new protections for millions of American workers that improves portability and continuity of health insurance coverage.

HIPAA includes protections for coverage under group health plans that limit exclusions for pre-existing conditions; prohibits discrimination against employees and dependents based on their health status; and allows a special opportunity to enroll in a new plan to individuals in certain circumstances.

HIPAA may also give you a right to purchase individual coverage if you have no group health plan coverage available, and you have exhausted COBRA or other continuation coverage.

## The Administrative Simplification Provisions of HIPAA

HIPAA's Administrative Simplification provisions require that every covered entity — health plans, health care providers, and health care clearinghouses — meet three basic requirements (among others).

These three basic requirements are:

- Privacy, which took effect in April, 2003;
- Transactions, which took effect October, 2003; and
- Security, which will take effect in April, 2005.

"The Final HIPAA security rule is broad, general and comprehensive," says Fusile. "It's scalable – in that not one size will fit all organisations. There are no pre-prescribed technology requirements (encryption, SSL, VPN, etc.). It doesn't tell you what you should do. Rather, it tells you what you should consider and allows each organisation to make its own determination as to what is appropriate for its particular situation."

## The Final Security Rule Summary

The summary of the security rule as stated by the Office of the Secretary, Department of Health and Human Services, says:

"This final rule adopts standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers. The use of the security standards will improve the Medicare and Medicaid programs, and other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information. This final rule implements some of the requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)."

## Good Security Practices for All Health Care Organisations and Beyond

"HIPAA is about good security practices for all health care organisations," adds Fusile. "These regulations by the U.S. Department of Health & Human Services apply not only to most U.S. health care plans, providers and clearinghouses, but also to many


(see next page)

*"What processes will your organisation put in place to help ensure that you have a well protected environment, as well as reputable and reliable vendors? And what measures will be kept in place to ensure that it stays that way?"*

*– Jeff Fusile, Partner-in-Charge, HIPAA Advisory Services, PricewaterhouseCoopers*

employee-sponsored health and welfare plans. This expansion outside of strict health care entities makes the HIPAA security rule particularly impactful on the corporate community and presents a new risk in an already highly regulated environment."

These HIPAA security guidelines may be the catalyst for a variety of questions for health care and non-health care entities to address, such as: How do you address the rules vs. what is required? How do you document these rules? And how often should you revisit those decisions?

## How HIPAA Security Is Different From Other Security

"The HIPAA Privacy rule gives us an understanding that covered entities must safeguard (secure) all identifiable health information held by a covered entity, no matter the form in which it resides," adds Cynthia Smith, a Director in PricewaterhouseCoopers' Global Risk Management Services Team in "HIPAA Security & Privacy Rules, Working Together, January 2002. "That includes protected health information maintained or communicated on paper, electronically, or orally."

"While the Privacy rule globally tells us what is required to protect all health information," says Smith, "the final Security rule will focus on what is required to safeguard protected health information in electronic form."

## The Three Core Categories Affecting Security

Pages 286-287 of the U.S. Department of Health and Human Services Summary discuss required updates to "review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information" for health plans, health care providers, and health care clearinghouses.

Specific security safeguards include:

**Administrative Safeguards**

| Standards | Sections | Implementation Specifications (R)= Required, (A)=Addressable | |
|---|---|---|---|
| Security Management Process | 164.308(a)(1) | Risk Analysis | (R) |
| | | Risk Management | (R) |
| | | Sanction Policy | (R) |
| | | Information System Activity Review | (R) |
| Assigned Security Responsibility | 164.308(a)(2) | | (R) |
| Workforce Security | 164.308(a)(3) | Authorisation and/or Supervision | (A) |
| | | Workforce Clearance Procedure | (A) |
| | | Termination Procedures | (A) |
| Information Access Management | 164.308(a)(4) | Isolating Health care Clearinghouse Function | (R) |
| | | Access Authorisation | (A) |
| | | Access Establishment and Modification | (A) |
| Security Awareness and Training | 164.308(a)(5) | Security Reminders | (A) |
| | | Protection from Malicious Software | (A) |
| | | Log-in Monitoring | (A) |
| | | Password Management | (A) |
| Security Incident Procedures | 164.308(a)(6) | Response and Reporting | (R) |
| Contingency Plan | 164.308(a)(7) | Data Backup Plan | (R) |
| | | Disaster Recovery Plan | (R) |
| | | Emergency Mode Operation Plan | (R) |
| | | Testing and Revision Procedure | (A) |
| | | Applications and Data Criticality Analysis | (A) |
| Evaluation | 164.308(a)(8) | | (R) |
| Business Associate Contracts and Other Arrangement | 164.308(b)(1) | Written Contract or Other Arrangement | (R) |



(see next page)

*"Remember," concludes Mr. Fusile, "many of the HIPAA privacy rule violations will be the result of poor security. So while the HIPAA security rules do not take affect for another year and a half, we need good security today to honor our privacy commitments."*

**Physical Safeguards**

| Standards | Sections | Implementation Specifications (R)= Required, (A)=Addressable | |
|---|---|---|---|
| Facility Access Controls | 164.310(a)(1) | Contingency Operations | (A) |
| | | Facility Security Plan | (A) |
| | | Access Control and Validation Procedures | (A) |
| | | Maintenance Records | (A) |
| Workstation Use | 164.310(b) | | (R) |
| Workstation Security | 164.310(c) | | (R) |
| Device and Media Controls | 164.310(d)(1) | Disposal | (R) |
| | | Media Re-use | (R) |
| | | Accountability | (A) |
| | | Data Backup and Storage | (A) |

**Technical Safeguards**

| Standards | Sections | Implementation Specifications (R)= Required, (A)=Addressable | |
|---|---|---|---|
| Access Control | 164.312(a)(1) | Unique User Identification | (R) |
| | | Emergency Access Procedure | (R) |
| | | Automatic Logoff | (A) |
| | | Encryption and Decryption | (A) |
| Audit Controls | 164.312(b) | | (R) |
| Integrity | 164.312(c)(1) | Mechanism to Authenticate Electronic Protected Health Information | (A) |
| Person or Entity Authentication | 164.312(d) | | (R) |
| Transmission Security | 164.312(e)(1) | Integrity Controls | (A) |
| | | Encryption | (A) |

"Every organisation really needs to do the assessment and risk analysis for its own company," continues Fusile. "A well planned and performed assessment can determine what it will cost and evaluate what the proper sequencing of implementation activities may be. If a solid assessment is not undertaken, organisations will likely spend far more than they should in the long run, and be far less secure."

Theoretically, a company can be fined if it is not in compliance with the proposed rules, but the greater risk appears to be a litigious one brought by an affected patient, member, employee, or worse, a class of these individuals. This could include instances where someone's privacy is violated.

"But there could even greater risk to a patient's data," says Ms. Smith. "For example, if a hacker breaks into a database of medical records, a company's data integrity could become suspect. A malicious change in a patient's prescription could cause an overdose, an allergic reaction, or other medical problems, including a patient's death."

"In a broader sense, look what happens when airport security is breached," adds Mr. Fusile. "One person runs through a checkpoint and thousands of passengers are evacuated. This analogy highlights the reality that significant costs are incurred because of one security mistake. Plus, it lets you understand that other industries are taking security, especially safety-related security, very seriously."

"Remember," concludes Mr. Fusile, "many of the HIPAA privacy rule violations will be the result of poor security. So while the HIPAA security rules do not take affect for another year and a half, we need good security today to honor our privacy commitments."

## For More Information

Visit www.pwc.com/hipaa, or download a practical analysis and guide for applying the final HIPAA Security Rule to your compliance efforts: PwC's Interpretation of the Final HIPAA Security Rule (as of 4/8/03), or contact Jeff Fusile, Partner, PricewaterhouseCoopers, 678.419.1558.

*"Management quickly realised that this represented a gap in their internal control structure and that action had to be taken to align, monitor, and report on the effectiveness of compliance with their security policies."*

*– Chris Miller, Partner, Security & Privacy Practice, PricewaterhouseCoopers*

# Vulnerability Detection Case Study: What We Did For A Packaging Manufacturer

## Description of Client's Business

This client is a leading manufacturer of packaging products operating worldwide, with employees in over 50 countries.

## The Client's Challenge

The company was experiencing significant growth through an aggressive acquisition strategy, recognising a substantial increase in sales and accompanying increase in employees globally. Its IT department was challenged with pulling together a cohesive information systems environment and security strategy that would support their rapid development efforts, new technology deployments and e-business initiatives.

Given the highly distributed IT organisation and infrastructure, it was top priority for the corporation's senior management to address information security policies, standards, monitoring, reporting, and compliance efforts. Results from periodic security assessments prompted management to pursue a more proactive approach to security policy management.

"Using their existing manual compliance testing methods," says Chris Miller, Partner, Security & Privacy Practice, PricewaterhouseCoopers, "it was extremely difficult for their management team to determine if their IT infrastructure was aligned to current security policies. Management quickly realised that this represented a gap in their internal control structure and that action had to be taken to align, monitor, and report on the effectiveness of compliance with their security policies."

## The PricewaterhouseCoopers Solution

The manufacturing company utilised PricewaterhouseCoopers' Integrated Security Policy Management Service to assist with developing a framework to align its security practices and IT technical controls to its corporate security policies.

"The company initiated a pilot Integrated Security Policy Management project that would provide a structured approach to implementing a solution," adds Miller. "This pilot enabled them to address high priority areas and also worked within their budget constraints. Symantec's Enterprise Security Manager™ (ESM) was chosen as the technology component to automate compliance testing and vulnerability assessment functions."

Using ESM as the data collection engine of the solution, the company developed an automated, centralised approach to discovering policy deviations and vulnerabilities across the applications, databases, operating systems, and servers.

The steps PwC took to solve this challenge included:

- Determining the information needs of each of the security stakeholders (e.g. senior management, IT and Security management) to design a solution to meet all requirements;
- Developing and piloting the automated policy management solution that integrated compliance testing tools (primarily ESM), extended existing IT operational processes, and established a sustainable reporting process for senior management;
- Deploying a reporting process to determine the baseline compliance with current security corporate security policies; and
- Establishing goals, targets, and timeframes for achieving compliance.

"Once the pilot was determined to be effective, the company then continued its work with PwC to establish the security policy management process definitions, related roles and responsibilities to ensure that security and technical controls stayed in compliance," continues Miller.

The combined project team developed a global rollout strategy and a phased



(see next page)

*The combined project team developed a global rollout strategy and a phased integration plan to support their global security policy management initiative. The company was able to formalise the roles and responsibilities for monitoring, reporting and compliance testing between the corporate security team and the technical support group.*

integration plan to support their global security policy management initiative. The company was able to formalise the roles and responsibilities for monitoring, reporting and compliance testing between the corporate security team and the technical support group.

### Benefits/Results to the Client

Benefits to the manufacturing company included:

- **The new role definition to share responsibilities promoted teamwork and collaboration** between the corporate security and technical support groups;
- **The new level of cooperation enabled the teams to leverage skills sets across the enterprise**, increase productivity, and reduce the human error that occurred from inconsistent security policy management processes;
- The custom reporting capability that was established in the pilot project provided **a simple method of reporting vulnerabilities and compliance issues across systems in different locations**;
- With the System Compliance Report narrative on management processes, the **senior management team now has the ability to quickly measure and report IT infrastructure compliance against established security policies** in a consistent manner across the enterprise;
- The management team now has an efficient and cost-effective process to **monitor compliance with their security policies, identify gaps in internal controls, and allocate resources to more strategic initiatives**; and
- With the tools and processes now in place, **the company has a sustainable solution that will help monitor internal security controls to reduce risk and exposure to vulnerabilities**.

"To date," says Miller, "the company has implemented and deployed their solution to all of their corporate locations in North America and Europe. They are now planning to extend the solution to the division level."

### For More Information

To learn more about how the Integrated Security Policy Management Service from PricewaterhouseCoopers can help your company manage vulnerabilities proactively, contact Chris Miller, Partner, Security & Privacy Practice, PricewaterhouseCoopers, 678.419.1206.

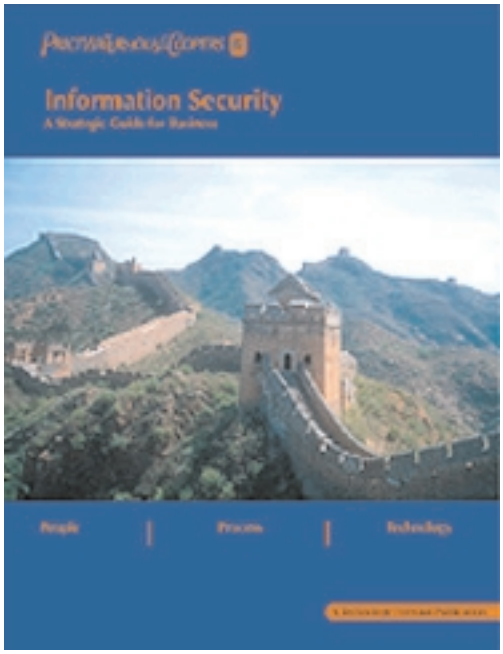
## *"Information Security: A Strategic Guide for Business"* — Defining Security's Emerging Role in Today's Organisations

This new book offers organisations a methodology for integrating highly effective security management techniques into everyday business processes.

The book is part of the PricewaterhouseCoopers' Technology and Risk Management Forecast series and includes a comprehensive overview of current and emerging security trends and technologies.

"*Information Security: A Strategic Guide for Business* provides business executives and security professionals with the latest thinking about information security challenges and best practices from one of the world's leading providers of information security solutions," says Allan Carey, program manager for Information Security Services Research, IDC. "Modern business leaders are finally beginning to understand that information security is not ensured through technology alone. This

(see next page)




*"Our clients look to us to provide them with a clear roadmap toward comprehensive, proactive, end-to-end security. Information Security: A Strategic Guide for Business, written by a global team of security experts from multiple disciplines throughout PricewaterhouseCoopers, represents our best thinking on security practices and procedures that will help organisations realise the true value and benefit of information security."*
*– Joe Duffy, Partner and Global Leader, Security & Privacy Practice, PricewaterhouseCoopers*

guide can help executives envision and embark upon a strategic approach to security that holistically integrates people, process, and technologies across the entire enterprise to create veritable end-to-end security."

This new book:

- Guides readers through the process of strategising, planning and implementing integrated security solutions that bring value to an organization;
- Showcases the emerging role security is beginning to play as a 'strategic enabler' of new business initiatives and compliance requirements;
- Investigates and discusses new trends and technologies across the security spectrum.

"Our clients look to us to provide them with a clear roadmap toward comprehensive, proactive, end-to-end security," says Joe Duffy, partner and global leader, Security & Privacy Practice, PricewaterhouseCoopers. *Information Security: A Strategic Guide for Business* was written by a global team of security experts from multiple disciplines throughout PricewaterhouseCoopers. It represents our best thinking on security practices and procedures that will help organisations realise the true value and benefit of information security."

## An Overview of the Book

*Information Security: A Strategic Guide for Business* includes comprehensive coverage of the following areas:

- **The Enterprise Security Business Model** — A detailed security strategy, planning, implementation, and maintenance framework to help companies align security with their overall business objectives.
- **Security Controls and Identity Management** — Business process control guidelines and techniques to improve authentication, authorisation, and access control so employees, partners and customers can get the information they need, when they need it.
- **Technology Infrastructure Security** — Insights on how to develop organisation-wide solutions and effectively use technology to enable the secure extended enterprise.
- **Threat and Vulnerability Management** — Ways to respond proactively to today's threat environment, including a comprehensive toolkit of technology and business process solutions.
- **Market Overview and Forecast** — Market leaders and innovators; the outlook for security software, hardware and services; and predictions by practitioners and thought leaders on the future of enterprise information security management.

## How To Order This Book

*Information Security: A Strategic Guide for Business* can be purchased for U.S. $49 by visiting www.pwc.com/tech-forecast/order
Or by calling +1.800.654.3387 (in the U.S. only) or +1.314.997.2540.
Or by sending a fax request to +1.314.997.1351.
American Express, MasterCard, and Visa are accepted.
Payment by check also can be arranged.

## For More Information

Download this brochure or contact Bryan Welch, 415.498.7991.

*Don't miss these important security events.*

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

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

### SECURITY CONFERENCES

### CISO Executive Forum

Sponsored by: PricewaterhouseCoopers, SPI Dynamics, ArcSight, Internet Security Systems
Date: Tuesday, December 9, 2003, 8:00 AM – 5:00 PM
Location: Jacob K. Javits Convention Center, New York City, NY
Register online at: http://ciso.issa.org/

The CISO Executive Forum is a concise, one-day event that will give InfoSecurity 2003 attendees a chance to explore the benefits of this new membership program and hear top industry professionals discussing today's most important topics. Admission to the CISO Forum is free for qualified security executives, and includes a continental breakfast, lunch and a special CISO Reception after the presentations.

### The Microsoft Government Security Summit East 2003

Date: December 2 - 4, 2003
Location: Washington Grand Hyatt, 1000 H. Street, NW, Washington, DC 20001

Register today – Space is limited! PricewaterhouseCoopers will be an exhibitor. Visit http://microsoft.com/usa/government or call 1-877-MSEVENT.
*Please enter the corresponding event code when registering.
Security is fundamentally important to the way government does business. Today's web-centric computing model demands that industry and government must change the way it thinks about security — from the Internet to internal networks. Microsoft is taking a leadership role in this effort. The 8th Annual Security Summit is designed to communicate Microsoft's commitment, strategies and product developments relating to security and reliability. Join members of Microsoft's development and security teams today to learn the steps Microsoft is taking to make software more secure in design, by default, and in deployment.

### UPCOMING WEBCASTS

### Hot Topic: Developing an Effective Approach to Patch Management

Sponsored by: PricewaterhouseCoopers and Microsoft
Featured Speaker: Brian Jensen, Senior Manager, Security & Privacy Practice, PricewaterhouseCoopers
Date: December 15, 2003
Time: 11:30am Pacific / 2:30pm Eastern
Duration: 1.5 hrs

Attend From Your Desktop! Join us for a current discussion of what's happening on the security patch management scene. Learn how your organization can develop an effective patch management strategy that is both scalable and sustainable.
Register Today At: http://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032239930&Culture=en-US

### ARCHIVED THREAT & VULNERABILTY WEBINARS

### Integrated Security Policy Management – Demonstrating Compliance and Security Controls For Your IT Infrastructure

Presented by: Harold Toomey, Product Manager, Enterprise Security Management, Symantec; Mike Cunning, Senior Manager, Security & Privacy Practice, PricewaterhouseCoopers


(see next page

*Join us at these upcoming industry events.*

View the recorded Webcast at your convenience. Instructions on how to access the archive:
Go to: http://www.placeware.com/cc/symantec/view?id+E-policy
Enter Your Name
Enter the Corresponding Recording ID ——> E-policy
Leave the Recording Key area Blank
Hit the View button

### ARCHIVED SARBANES-OXLEY WEBINARS

**Microsoft Executive Circle Presents: How does Identity Management Support Sarbanes-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
URL for viewing: www.microsoft.com/usa/webcasts/ondemand/2141.asp

**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, Global Risk Management Solutions, at bryan.r.welch@us.pwc.com, 415.498.7991.