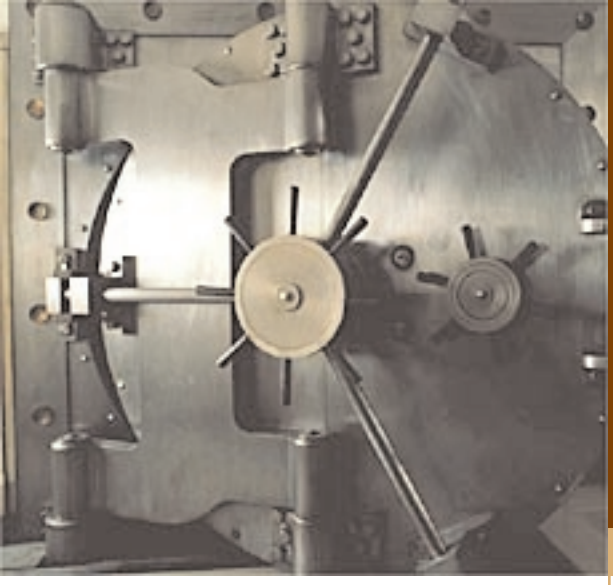


PRICEWATERHOUSECOOPERS

The Secure Solution

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

VOLUME 17, JULY/AUGUST 2003

In This Issue:

This edition of The Secure Solution, a monthly newsletter from the Security & Privacy Practice of PricewaterhouseCoopers, includes the following: an overview of our recently realigned, redefined and redesigned Website; a summary of our latest Sarbanes-Oxley White Paper; a look into the top five privacy issues for using mobile devices; a Data Quality 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

The Security & Privacy Solutions Website: Realigned, Redefined and Redesigned With the ESBM™

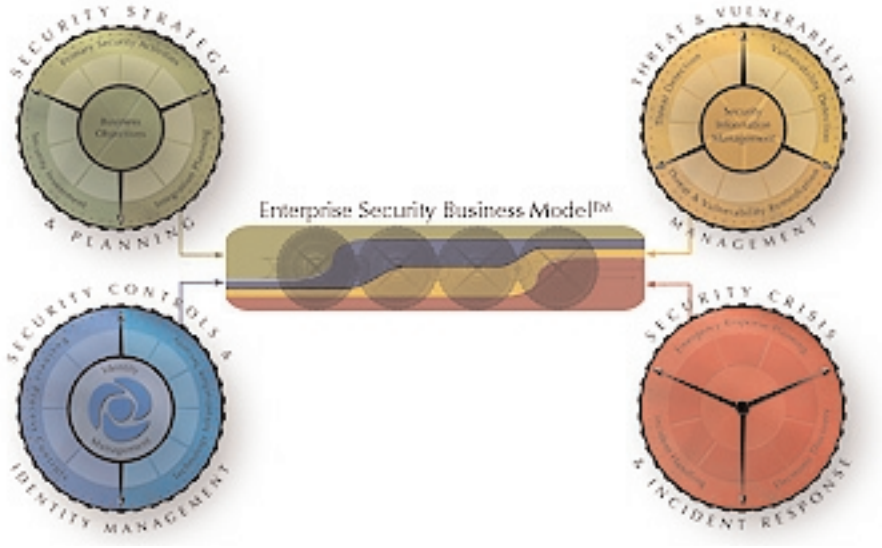
Over the past six months in *The Secure Solution*, we've offered detailed articles about PricewaterhouseCoopers' vision of end-to-end security: the Enterprise Security Business Model (ESBM)™.

Its four distinctive stages: Envision, Engineer, Operate, and Respond show the process that identifies, creates, captures and sustains the value of security in an organisation, and reflect our belief in empowering clients to meet their security-related objectives.

Explore our Range of Security & Privacy Solutions

Now, we're proud to announce our realigned, redefined and redesigned Security & Privacy Solutions Website that mirrors PwC's comprehensive, integrated suite of solutions. Each is aligned with the Enterprise Security Business Model™. And each is individually tailored to meet your company's unique security and privacy requirements.

This graphic displays how our solutions overlap and interconnect with the ESBM:



Each of the four solution areas that comprise the Security & Privacy Solutions Suite is described below, with links to more information on the website.

Security Strategy & Planning – The Security of Strategic Alignment

In a world of limited time, money and resources, how you can balance the two competing priorities of protection and enablement?

(see next page)

We're proud to announce our realigned, redefined and redesigned Website that mirrors PwC's comprehensive, integrated suite of Security Strategy & Planning solutions.

"Our Security Strategy & Planning Solutions help forward-thinking companies develop a sensible, strategic plan to leverage the Internet, to deploy new security Web applications," says Mike VanDemark, senior manager, PricewaterhouseCoopers Security & Privacy Practice. "These solutions can help an organisation expand information technology infrastructures — creating a security strategy to focus resources in full alignment with your business objectives."

By deploying the Security Strategy & Planning Solutions, benefits to your enterprise include:

- Resource optimisation through effective allocation;
- Capital and operating cost reductions;
- Faster delivery times via reusable methods and technologies;
- Better control via implementation of a key security management metric;
- Improved security through articulation of security ownership and accountability.

This highly effective suite of services is developed and refined to help you establish every component of a total security solution. It encompasses:

- Security Strategy & Roadmap Development;
- Security Awareness & Training;
- Security Policy & Procedure Development;
- Enterprise Security Architecture Services (ESAS);
- Security Framework Gap Analysis; and
- Security & Privacy Compliance.

Security Controls & Identity Management — The Security of Inclusion

Security Strategy & Planning is just one component of PricewaterhouseCoopers' comprehensive solution set. The second is Security Controls & Identity Management.

"Because of growing concerns globally with news issues such as identity theft, ensuring the right people gain controlled access to your resources, and gaining a single view of a user across your enterprise, this is perhaps the fastest growing area of security worldwide," continues Mr. VanDemark.

PwC's Security Controls & Identity Management Solutions specifically target your enablement requirements by helping you access information assets through integrated solutions focused on identity management, business process controls and technology infrastructure. Benefits to your enterprise include:

- Reduced operating costs;
- Increased productivity;
- Higher customer satisfaction;
- Improved business management; and
- Stronger security.

A proprietary tool within this solution is the Identity Management Value Calculator. PwC engaged The Meta Consulting Group to create this directional tool for decision making using benchmark data from a survey on identity management. Many companies earn a return on their investment in an Identity Management solution in one to three years.

The Security Control & Identity Management suite of services includes:

- Identity & Access Management;
- Business Process Controls;
- Technology Infrastructure Security;
- ERP Controls Integration;

(see next page)

Each of the four components is described here, with links to its separate pages among the overall site, specific benefits, proprietary tools, and what each component comprises.

- SAP Security Administration (SAFE); and
- Data Management.

Threat & Vulnerability Management — The Security of Exclusion

Just as important as allowing online access to the right people is the problem of keeping the wrong people out of your website. This poses other questions. One is how do you do this while continuing to manage your complex environment? Another is how do you stay ahead of the vulnerability curve? A third question is how do you get a real-time snapshot of your security posture that's integrated, organised and cost-effective?

"Our Threat & Vulnerability Management Solutions specifically target your protection requirements," says Mr. VanDemark. "They help you integrate prevention, detection and correction technologies through a 'security dashboard' approach that helps you monitor and manage heterogeneous security performance metrics and indicators."

Benefits to your enterprise by integrating these solutions include:

- Reduced likelihood of business interruption from a security-related event;
- Reduced impact of unanticipated events through detection, reaction and containment techniques;
- Reduced overall cost of ownership by leveraging the optimal combination of resources — people, process and technology — to meet your organisation's specific requirements;
- Enhanced capability to correlate events from data emerging from multiple security touch points;
- Full support from a comprehensive inventory of known exposures in the technology environment; and
- Improved ability to demonstrate compliance with regulatory and best practice requirements.

In addition, PwC's Threat & Vulnerability Management Solutions can deliver a range of world-class protection services, including:

- Threat Detection;
- Vulnerability Detection;
- Threat & Vulnerability Remediation; and
- Security Information Management.

Security Crisis & Incident Response — The Security of Controlled Response

The fourth and final Security & Privacy Solution set answers the critical question no organisation wants to ask, but many must: How can you quickly respond when your critical information is compromised by a security breach?

"The Security Crisis and Incident Response services can help you 'stop the bleeding' as an incident occurs and stabilise your organisation," concludes Mr. VanDemark. "This service is designed to assist you during and after a security-related event. It also helps you plan ahead by establishing crisis response policies and procedures. This service can take you from a reactive "fire drill" response to a proactive way of dealing with security threats and vulnerabilities."

Benefits to your enterprise through management, process and technical expertise includes:

- Effective planning for security events;
- Reduced event impact through fast, efficient repair and investigation;
- Cost containment and asset recovery through cost-effective digital forensic capabilities; and
- Access to expert witness services to support matters of litigation.

(see next page)

The Sarbanes-Oxley legislation offers a unique opportunity for the accounting profession to move to a higher level, to be, in effect, the vanguard of corporate reform.

Because networked computing is at the heart of every modern enterprise, vigilance is paramount. PricewaterhouseCoopers' Security Crisis and Response services include these cost-effective, comprehensive crisis solutions:

- Security Crisis & Response Policy and Procedure Development;
- Cybercrime Incident Response Teams;
- Digital Forensics; and
- Expert Witness Services.

To Find Out More

For more information about each of these solution sets, please contact us at risk.management@us.pwc.com or call our hotline at 1.800.639.7576.

The Sarbanes-Oxley Act of 2002: Understanding the Independent Auditor's Role in Building Public Trust — A White Paper

Since the Securities and Exchange Act of 1934 was passed, a system of guardianship has served the public well for certain bookkeeping and reporting responsibilities. But recent corporate scandals called its efficacy into question. Furthermore, investor trust in corporate reporting has dramatically eroded.

As with many systems of checks and balances, time and pressure have impacted the Exchange Act 's effectiveness. Today, nearly 70 years later, we have a fiercely competitive business climate with a high-stakes global marketplace vying for investor capital.

The Third Sarbanes-Oxley White Paper: A Summary

This just-published PricewaterhouseCoopers White Paper is entitled "The Sarbanes-Oxley Act of 2002: Understanding the Independent Auditor's Role in Building Public Trust". The third publication in our Thought Leadership series, the White Paper:

- Focuses on the ways in which the recent legislation affects those in the public accounting profession. It also discusses how this, in turn, impacts others in the Corporate Reporting Supply Chain.
- Explores the obligations of the independent auditor in the Corporate Reporting process — as mandated by Sarbanes-Oxley and subsequent rules.
- Analyses and communicates PricewaterhouseCoopers' understanding, as leaders in this profession, of the relevant aspects of this important legislation and its pertinence to our role in this chain.
- Examines changes in the following key areas:
  - Strengthening auditor independence;
  - Increasing the depth of audit services and the value of the audit to shareholders; and
  - Establishing new oversight for the auditing profession.

The Evolving Role of the Independent Auditor

It has become clear to investors and the public alike that the auditor 's role must be strengthened. The Sarbanes-Oxley 2002 legislation offers a unique opportunity for the accounting profession to move to a higher level — to be, in effect, *the vanguard of corporate reform*. It is an opportunity and a challenge both warranted and welcome.

This White Paper reveals the opportunities, in selected areas, for management, audit

(see next page)

As of today, the wireless industry is not yet offering its customers a privacy policy that provides choices as well defined as the financial industry's.

committees and our profession to go beyond current requirements to achieve a deeper level of transparency in corporate reporting, and to implications of the new independent oversight of the accounting profession.

Stand and Be Counted

The authors of this White Paper believe it is time to stand and be counted. Company stakeholders are demanding a business environment distinguished by the principles of *transparency, integrity and accountability* – and characterised by a true state of independence. These reforms have not been entered into lightly. Nor should they be taken lightly in return. Rather, they must be acknowledged, accepted and fully complied with, in the spirit in which they were intended.

We are among those in the profession who believe these changes will prove essential to supporting a healthy, effective corporate reporting supply chain — and thus to the rebuilding of investor trust in the capital markets.

Download this White Paper

To read this White Paper now, download it today.

The Top Five Privacy Issues In A Mobile World

"The Secure Solution" recently interviewed Ruth V. Nelson, Director, PricewaterhouseCoopers, regarding the continuing concern of privacy issues with wireless communications devices and services.

Banks, credit card companies, stock brokerages and automakers today are offering customers like you an opt-out program within their corporate privacy policies. Specifically, these programs explain how you can prevent the sharing of your personal data with other companies. Making a phone call, or sending a letter, can remove you from the mailing lists that a company may share with or sell to other companies.

Yet as of today, the wireless industry is not offering its customers a privacy policy that provides choices as well defined as the financial industry's.

Mobile Privacy is an Issue of Growing Concern

The telecommunications industry, through the Cellular Telecommunications & Internet Association (CTIA), realised the pending wireless privacy issues through their creation of Location Based Privacy Principles in November, 2000. Attempts to have these principles validated by the Federal Communications Commission, however, proved unsuccessful. There are voluntary Wireless Advertising Association Privacy Guidelines, such as not condoning wireless push advertising without explicit subscriber permission, but we don't have officially sanctioned standards established at this time.

Wireless privacy is an issue. The data itself is growing exponentially because of the increasing numbers of wireless devices — commercial wireless networks, cell phones, smart phones, laptops, PDAs, pagers, GPS, even smart tags (RFID – radio frequency identification) in clothing. In fact, on July 9, CNET News.com said that executives of Wal-Mart, the world's largest retail chain, are focusing on installing RFID systems in its warehouses and distribution centers.

To set the scene in defining privacy issues, the requirements are usually framed as individuals should have a right to:

- Control the information collected;

(see next page)

How Some Companies Are Violating Your Privacy

Two companies have recently created a tremendous backlash for violating their user's privacy.

First, a Japanese wireless company introduced countermeasures to a mobile phone scan, which is known in Japan as "wangirl" (one ring and cut). A computer, using hundreds of phone lines, dials random mobile phone numbers. After one ring, the call hangs up, but leaves the number stored in the receiving party's mobile phone. If the person returns the call, they're connected to a sales tape soliciting business, and sometimes sex services. Even worse, the person is usually charged at premium rates for the call by the marketing solicitor.

Not only is the scam proving to be a major irritation for mobile phone users in Japan, but it's also disrupting business. Twice during August 2002, the phone lines in Osaka and surrounding areas have been jammed because of the scam.

Second, a US-based rental car company tried to use emerging GPS technology to its advantage. It provoked a lawsuit from an angry customer and created a flurry of negative publicity.

The company equipped some of its cars with GPS and software to locate a lost or stolen car, plus provide maps and directions. But when the company enhanced the system to track and report each car's speed, they crossed the line. Customers were allegedly told of the system's capabilities (and notified by boldface type in the rental agreement), and that they'd be fined $150 each time they traveled faster than 79 mph for more than two minutes.

But one customer, shocked to find that the company had deducted $450 from his bank account for violating the speeding clause, complained to its home state's Department of Consumer Protection. The complaint brought a cease-and-desist order against the company for failing to provide adequate notice and for extracting a fee when no "damage" to the company had been shown.

The Department ruled that this company's application of the MLS technology was inappropriate and ordered it to stop using the system to track customers' speeds. The company had to refund about $13,000 of the fines.

- Control how the information is used;
- Control third party access to the information; and
- Access and correct personal information.

These concepts are still yet to be fully implemented transparently across the wireless service and information cycle.

Wireless Device Use Is Expanding Exponentially

In addition, the value of the information is increasing. Numerous data categories can now be combined that include: location, profile, experiential, and community (who we call). The sheer amount of data that can be amassed continues to rise as enterprises are using more data. According to Gartner, there will be 1.5 billion mobile subscribers predicted worldwide by 2005. By 2008, any device enabled for wireless communication will sense location and be traceable to within 20 meters.* So retailers and wireless enterprises will eventually try to micro tag an individual to a specific location, as seen in Steven Spielberg's movie, 'Minority Report'.

Can retailers make money from this? Eventually. Do we know if consumers will tolerate this? That depends on the benefits versus the individual costs to personal privacy. The public at large is still generally unaware there's such a great profiling capability and how many companies will pay for your data, including your buying habits, even your family profile. However, advocacy groups are doing their best to raise awareness within the public, and to educate regulators more effectively.

Enterprises need awareness of their risk and vulnerabilities, strategies for overcoming the risk, and concrete actions with measurable results.

Who Are You Contracting Your Privacy With?

From a controls standpoint, most of these wireless devices are IP-enabled and connect to an IP network. It's feasible that a cell phone can connect over the Internet to a computer. Similarly, PDAs, cell phones and pagers have immature operating systems that have rudimentary access controls, security or privacy. Basically, a business user's privacy is not yet adequately protected with these devices, let alone a general consumer.

The Top Five Mobile Privacy Issues

If individuals could decide how to best control their privacy for using wireless devices, Ms. Nelson believes the key issues include:

1) **Controlling the devices to enable privacy** — More and more devices are being used in business with inadequate security, so enterprises have to make them more secure. Many companies don't currently believe they need to set up privacy firewalls or policies to protect a device, but they should.
2) **Enabling individuals to turn their privacy choices on and off** — This could allow you to have technology-enabled choices to block your location, block messaging, choose vendors or communication paths. If you think that micro tagging an individual to a specific location in a store or retail environment is too intrusive, turning the privacy choices on or off can let someone exercise their choices. Key question: How do we develop privacy-enabled technology that is future-proof?
3) **Resolving the issue of letting the user know which privacy statement is governing the device, the data and the services** — Users deserve to know — in plain English, not legalese — what their privacy choices are throughout the communication chain that can involve numerous parties from the device manufacturer, the telecommunications provider, the PDA applications, the Internet Service Providers, and the Websites. Which privacy statement governs these interactions?
4) **Drawing the line for deploying forensics to extract personal information on a mobile device used across a corporate LAN** — Where do we draw the line

(see next page)

Consumers should be provided with informed choices as to how their personal data is used by their telecom, information and media providers.

between using forensics to uncover your personal data on a mobile device versus your company information? How do you recognise and protect that personal information when you connect through another device on a corporate network, such as a calendar app, email, or other data?

5) **Discussing standards for privacy principles** — Mobile and wireless computing offers unique, exciting new application and data capabilities. But mobility also introduces new challenges to privacy. Because existing laws and regulations don't offer enough protection, the key players in the telecommunications, information and media industries should consolidate and agree upon privacy standards and principles.

The Bottom Line

An April 4, 2003 Gartner Strategy, Trends & Tactics online article entitled "U.S. Enterprises Should Prioritize Privacy Management" by Walter Janowski raises the red flag. "U.S. enterprises face customer backlash and government intervention regarding privacy concerns," says Janowski. "To mitigate these risks, they must overcome internal indifference and limited vendor interest in delivering solutions."**

He's not alone. Among others, Ms. Nelson strongly believes that consumers should be provided with informed choices as to how their personal data is used by their telecom, information and media providers. If the financial industry already has legislated policies in place, shouldn't mobile device manufacturers and media providers also be allowed to standardise their privacy policies for their respective customers?

For More Information

To find out more about privacy issues, please contact:
Ruth V. Nelson
Director
PricewaterhouseCoopers
646.471.8991

* Source: Gartner Research Note
Title: Mobile Location Service Market: Drivers and Obstacles
Author: M. Basso
Publication Date: 19 July 2002

** Source: Gartner Strategy, Trends & Tactics
Title: U.S. Enterprises Must Prioritize Privacy Management
Author: Walter Janowski
Date: 4 April 2003

(see next page)

The client was able to learn which areas were most at risk in its conversion and obtained recommendations for minimising that risk on later implementations.

Data Quality Case Study: Pre-Implementation Data Conversion Review Identifies Exposure

Description of Client's Business

The client is a large U.S. distributor of industrial, medical and specialty gases, welding, safety and related products.

The Client's Challenge

The client asked PricewaterhouseCoopers Data Management Group (DMG) to conduct a pre-implementation data quality/conversion review.

The company needed to assess the key process controls and related risks associated with the implementation of its Oracle financial modules including: General Ledger, Accounts Payable, Fixed Assets and System Administration.

In addition, the company's Internal Audit Services department was doing a conversion review, but it didn't have the staff or the technical expertise to do the job on its own.

The PricewaterhouseCoopers Solution

"PwC was asked to assess the key process controls and related risks associated with implementation of four Oracle modules," says Stephen Eddy, Partner, PricewaterhouseCoopers' Data Management Group.

"We interviewed key personnel and reviewed relevant source documentation," adds Ganesan Balaji, Manager, PricewaterhouseCoopers' DMG. "Next, we assessed the data conversion planning/organisation and the conversion inventory for adequacy of methods used to identify the required data conversions. Strategies and decisions regarding the selection of legacy data and methods/methodologies of data mapping were also reviewed. Plus, PwC assessed the overall strategy and responsibility for data cleansing and purging. We then reviewed the plans for data reconciliation."

Benefits/Results to the Client

As a result of our work, the client was able to learn which areas were most at risk in its conversion and obtained recommendations for minimising that risk on later implementations. This included:

- Increased data quality from legacy systems — Data extracts were obtained from the legacy systems. Integrity tests were also performed on a sample basis to evaluate whether the data would meet the increased quality required by an integrated systems operating environment. For example, we identified duplicate vendors and inaccurate address information, such as invalid state and zip codes.
- Identified areas for process improvements — In our findings, PwC identified areas for control and business process improvements. We also identified a need for vendor de-duplication and normalisation, as well as correction of invalid vendor address information.

Contact Us

To find out more about PricewaterhouseCoopers' Data Quality offering, please contact:

George Marinos
(US) +1 646 471 8861

(see next page)

Join us at these upcoming 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

To be announced…

ARCHIVED IDENTITY MANAGEMENT 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

The Sarbanes-Oxley Act of 2002 establishes new or enhanced standards for corporate accountability and penalties for corporate wrongdoing. Learn what Sarbanes-Oxley means to CIOs and explore how improved security – through Identity and Access Management solutions – can help.

URL for viewing: www.microsoft.com/usa/webcasts/ondemand/2141.asp

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

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

WANT TO KNOW MORE?

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