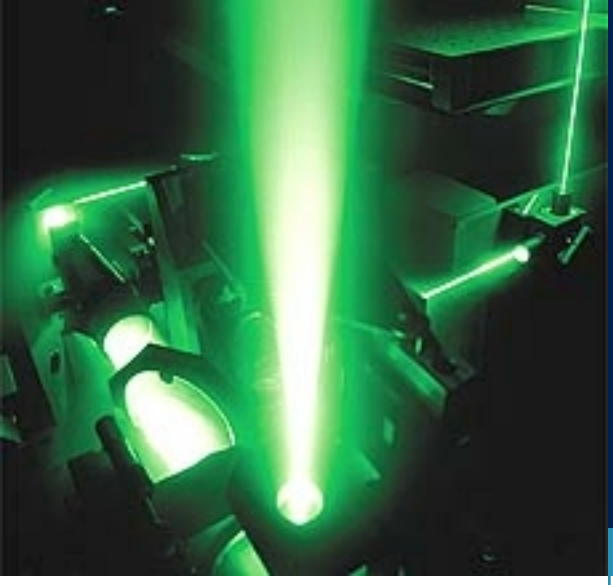


PRICEWATERHOUSECOOPERS

Tech Spotlight

A Focus on Security, Technology and Data Services

A monthly newsletter brought to you by PricewaterhouseCoopers' Technology and Data Services Practice: IT Business Risk Management... Data Management... Security. Integrating people, process and technology across your enterprise.

VOLUME 27, JUNE 2004

In This Issue:

For questions about our newsletter, or our Security, Technology or Data Services, please contact one of our marketing professionals.

Who To Contact:

James F. Kelly
Americas Marketing Leader
Advisory
PricewaterhouseCoopers
415.498.5376
james.f.kelly@us.pwc.com

Kate Oliver
Marketing Director
Technology & Data Services
PricewaterhouseCoopers
860.241.7333
kathryn.oliver@us.pwc.com

Identity Theft and Security Breach Notifications: *Reporting on Request*

The editors of "Tech Spotlight" often receive requests from readers about topical storylines. This is the latest in our series of articles prompted by suggestions from our audience.

Imagine someone at your bank having his/her laptop computer stolen, containing hundreds of thousands of customer database records.

Then imagine receiving a letter from your bank that reads: "I am writing to you because a recent incident may have exposed you to identity theft." It would further inform you that either your credit card, financial account, Social Security or Driver's License number has been compromised, then list the steps that you should take to further protect yourself. [1]

To date, half a dozen leading US financial institutions have sent these notification of security breach letters to tens of thousands of their customers. However, some bank customers have not been notified of these thefts until weeks after the incidents have occurred. California's new Financial Breach Notification Act now mandates prompt notification." [2]

If you should receive such a letter in the near future, your mind may spin about what your next steps should be, Close your checking account? Destroy your credit card? Change banks? Get a new Driver's License? Or all of the above?

The rapidly growing problem of identity theft acted as a catalyst for security breach notifications. We asked two privacy experts — Alex Fowler and Ruth Nelson, Co-Leaders of PricewaterhouseCoopers' Privacy Practice, to respond with a point of view on identity theft and possible solutions for both individuals and financial institutions.

Identity Theft Is On the Rise

Both Mr. Fowler and Ms. Nelson agree that identity theft is spiraling out of control. "This is an ever-increasing issue of the computerised information age," says Mr. Fowler.

- Fact: Two laptops have been stolen from a major West Coast bank in the last six months containing Social Security numbers, loan and credit card information for hundreds of thousands of customers. [2]
- Fact: The FTP server of a large collector and processor of consumer information was reportedly accessed and downloaded — while data was being exchanged with its biggest clients — by an intruder who had broken into the company's massive database. [3]
- Fact: A Federal Trade Commission survey of September 3, 2003 found that **27.3 million Americans have been victims of identity theft in the last five years**, including 9.9 million people in 2002 alone. According to the survey, 2002 identity theft losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion in out-of-pocket expenses. [4]

(see next page)

To date, half a dozen leading US financial institutions have sent these notification of security breach letters to tens of thousands of their customers.

- Fact: **A July 2003 survey showing** that 33.4 million Americans say they have been victims of identity theft or fraud since 1990, **with over 13 million since January 2001 and rising**. designed by Dr. Alan Westin, Professor Emeritus of Public Law and Government at Columbia University, funded by Privacy & American Business P&AB) and conducted by Harris Interactive.[5]
- Fact: According to the California Department of Consumer Affairs' "Recommended Practices on Notification of Security Breach Involving Personal Information," **the number of identity thefts is "nearly 10 times greater than the previously quoted estimate of less than a million a year.** If the same rate is applied to California, then over a million Californians became victims of identity theft in the past year." [1]
- Fact: Identity theft doesn't stop at the US borders. ID theft and fraud levels are now quite high in Canada, Australia, and Britain, and are developing in Japan, with quite similar costs to victims and businesses. [1]

Identity theft affects all incomes and all races, in urban and suburban areas, in every corner of America.

The Cause of Breach Letters

According to a request for comments published August, 2003, in the *Federal Register* by the bank regulatory agencies on a document titled, "*Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*," breach notification should be given when:

- "An employee of the institution has obtained unauthorised access to sensitive customer information maintained in either paper or electronic form;
- A cyber intruder has broken into an institution's unencrypted database that contains sensitive customer information;
- Computer equipment such as a laptop computer, floppy disk, CD-ROM, or other electronic media containing sensitive information has been lost or stolen;
- An institution has not properly disposed of customer records containing sensitive customer information; or
- The institution's third party service provider had experienced any of the incidents described above, in connection with the institution's sensitive customer information." [6]

Sometimes, breach letters inform customers of thefts of private information, but later, it was determined that no data was actually misused. A January theft of a company that processes financial transactions mostly for air travel was the victim of a burglary of two computers. The company "made the appropriate notifications commensurate with the theft and… the necessary steps are being taken." [7]

In addition, "a major bank," notes Ms. Nelson, "has actually sent end-of-the-year tax statements (1099s with Social Security numbers) destined for nearly 4,000 of its customers **to the wrong parties**." The institution said it was because of an isolated printing error.[8]

"Organisations have been hacked and identities have been pilfered," she continues. "What has been stolen and how has it been compromised may initially be undetermined. We always have to discover what's the likelihood of that data enabling a hacker or criminal to do something malicious with the identities?"

California-Hosted Bill Urges Prompt Notification Nationwide

Senator Dianne Feinstein of California has introduced a bill, now before the US Congress, using California's 2003 bills (SB1386/AB700) as a model. If passed, it would mandate notification of customers affected if a database is broken into and personal data is compromised.[2]

According to a PricewaterhouseCoopers publication, *California SB1386 and AB700:*

(see next page)

Where Consumers Can Go for Help

The National Security Breach Notification Act is tied directly to helping people get the information they need when their identities are compromised. You can find out more at these sites:

- Federal Trade Commission's Identity Theft Hotline toll-free, 1-877-IDTHEFT (438-4338);
- www.ftc.gov.

Disclosure of Personal Information Act Legislation White Paper, the California Bills were introduced to Sacramento by Senator Steve Peace (Democrat, El Cajon) and Assemblyman Joe Simitian (Democrat, Silicon Valley). The bills were the result of a breach of personal information at the State Controller Office, where an attack may have allowed a hacker or hackers access to payroll information for all 265,000 full- and part-time state employees' information, including first initials, middle initials, last names, Social Security numbers and other payroll information. [9]

The White Paper states, "Though the breach occurred on April 5, it was not discussed until May 7, 2003. Senator Peace and Assemblyman Simitian were upset with the event, but were 'appalled' that the Controller's Office knew of the attacks and decided not to inform employees for several weeks."

The Disclosure of Personal Information Act (California SB1386/AB700) states that if any business or state agencies within California have a security breach, "the disclosure must be made in the most expedient time possible without unreasonable delay to any individual person" — by written, electronic and substitute notification. [8]

"I think the Security Breach Notice Law has the potential to have a very big impact on preventing identity theft in two ways," says Joanne McNabb, Chief of the Office of Privacy Protection, California Department of Consumer Affairs. " First, and the most important, it is an incentive for organisations to really tighten the security with which they protect consumers' identities. Second, in cases where there are breaches, it gives potential victims an early warning so they can better protect themselves."

Proactive Corporate Measures from PricewaterhouseCoopers

"The issue of identity theft is directly impacting consumers in a new way," says Ms. Nelson. "It's created a proposed law triggering corporations to notify and inform its customers. Following California's lead, identity theft has also acted as a catalyst as other states with similar legislation drafted for approval."

"At PricewaterhouseCoopers," she continues, "we believe that national notification requirements will become law very soon. In the Financial Services industry, we already have Proposed Interagency Guidance on Response Programs for Unauthorised Access to Customer Information and Customer Notice.

"The bottom line is that an organisation needs to take proactive physical and logical security measures to secure and protect customer information within the entire extended Information Management cycle that includes internal and vendor systems. This involves both having accurate Customer Information Inventories and Dataflows, appropriate controls and audit trails, and an accurate Threat and Vulnerability Risk Model. Lastly, organisations must implement rapid response teams when breaches and compromises occur to not only meet notification time limits, but more importantly, protect and reassure customers and minimise brand impact."

Organisations may look to a comprehensive approach, such as PwC's Enterprise Security Business Model™ (ESBM™), a detailed, end-to-end view of security, which shows the process that identifies, creates, captures and sustains the value of security in an organisation. The ESBM reflects PwC's belief in empowering clients to meet their security-related objectives to help prepare your environment for new and existing regulatory requirements such as BS1386 and AB700.

According to the new California law — and the proposed national bill — if there is a security breach, the company must:

- Determine who and what has been compromised, what they should do next, and how the breach ultimately affects each of its customers. "This can be an inter-related, complex system of notification that's still evolving where multiple institutions and vendors can sometimes be involved," adds Ms. Nelson.
- Investigate the potential breach and determine the extent of impact to its

(see next page)

Five Steps to Take If You Receive a Breach Notification Letter

If you believe your identity has been stolen — or should you receive a Breach Notification Letter — here are the top five steps you should take, according to the Federal Trade Commission and the California Department of Consumer Affairs:

1) Send a copy of the Breach Notification letter to any companies that are affected by your identity theft, including banks, airlines, grocery and retail stores, gasoline companies, plus law enforcement agencies.
2) Contact the three major credit bureaus. Call any one of the numbers below and ask a credit bureau to place a fraud alert on your credit file, requesting that creditors contact you before opening new accounts or before making any changes to your existing accounts. NOTE: The other two credit bureaus will be automatically notified to place fraud alerts by the one you contact, and all three credit reports will be sent to you — free of charge. Equifax 1-800-525-6285; Experian 1-888-397-3742; Trans Union 1-800-680-7289
3) Carefully review your credit reports. Read the reports for accounts you don't recognise, especially if any accounts have recently been opened. Pay particular attention to the inquiries section for names of creditors from whom you have not requested credit. Be aware that some companies may bill under names other than their store names; the credit bureau will be able to explain that to you when this is the case.
4) Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit when you dispute new unauthorized accounts.
5) File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.
6) File your complaint with the Federal Trade Commission. It maintains a database of identity theft cases used by law enforcement agencies for their investigations. By filing a complaint, it helps them learn more about identity theft and the problems victims are having to better assist you.

customers by geographic region. In certain cases, this will involve law enforcement agencies. "As soon as a company identifies a breach through its network or of its customer data, it must then re-create the scenario or incident to identify the facts and implement procedures to remediate and prevent that threat from reoccurrence. Where vendors are involved — right to audit — clauses should be invoked," says Ms. Nelson.

- Where the breach conditions are met they must then provide notice to their customers (if no law enforcement exemption exists), and consider notifying all other customers potentially impacted by the breach. "This law prevents organisations hiding breaches anymore. It's resource intensive, it's costly to organisations, and it impacts their brands negatively."
- Review policies, procedures, and preventative controls in light of facts of the incident, implement self-audits and look at refreshing training and awareness.

"Corporations are being forced to take their security and privacy practices to the next level of real-time knowledge of where Customer Data resides and what threats and vulnerabilities exist," she concludes. "PricewaterhouseCoopers offers its clients a range of Security and Privacy Solutions, such as Risk Assessments, Patch and Event Management, Policy and Procedure Management, Vendor Management, Security Framework Gap Analysis, Security Awareness & Training, as well as Security & Privacy Compliance Programs."

Find Out More...

To find out more about how to protect yourself from Identity Theft, please contact Joanne McNabb, Chief, Office of Privacy Protection, California Department of Consumer Affairs. 866.785.9663, www.privacy.ca.gov

To find out more about privacy issues regarding identity theft breach notifications, contact Ruth Nelson, 1.646.471.8991, or Alex Fowler, 1.415.498.7590, Co-Leaders, Privacy Practice, PricewaterhouseCoopers. Or download the PricewaterhouseCoopers White Paper: California SB1386 and AB700: *Disclosure of Personal Information Act Legislation*.

[1] "Recommended Practices of Notification of Security Breach Involving Personal Information", October 10, 2003, Joanne McNabb, Chief, Office of Privacy Protection, California Department of Consumer Affairs, www.privacy.ca.gov

[2] "Wells Fargo Does It Again," www.identitytheft911.com, 16 April 2004.

[3] "Axciom Database Hack Highlights Risk," Linux Insider, www.TechNewsWorld.com, Part of the ECT News Network, by Jay Lyman, 08/11/03.

[4] "FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers", Press Release, September 3, 2003.

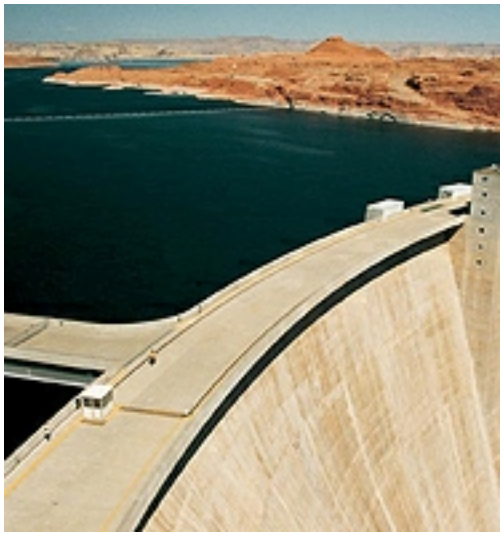
[5] "Privacy & American Business Survey Finds 33.4 Million Americans Victims of ID Theft; Consumer Out-Of-Pocket Expenses Total $1.5 Billion A Year," Press Release, July 30, 2003.

[6] "ID Theft Response Program Proposal," Banker's Online, August 14, 2003.

[7] "Airline Ticket Processor Reports Computer Theft," Washington Post, Griff Witte, January 14, 2004.

[8] "Bank of America Sends 1099 Statements of California Customers to Wrong Addresses," ISSN, Volume 3, Number 4, January 26, 2004, Page 85.

[9] PricewaterhouseCoopers White Paper: California SB1386 and AB700: Disclosure of Personal Information Act Legislation.



When 15 kilobytes of malicious code is more widely recognised by name than the top three global CIOs, then patch management — together with other critical information security issues — has effectively crash-landed onto the boardroom agenda.

The Discipline of Enterprise Patch Management — A Critical Component of A Broader Approach to Protection: A White Paper

On the morning of January 25th, 2003, the economy of South Korea was brought to a screeching halt by a malicious string of code called Slammer. Even as the worm raced across the Pacific to disable 13,000 automated teller machines in the U.S. (each proudly displaying the brand of its corporate owner, a globally prominent retail bank) — Nimda and Code Red were already household names around the world.

What makes news stories like this sobering for corporate executives is not just that Slammer, Nimda and Code Red — and all the newsworthy worms in the first half of 2004 — were highly successful attacks that cost businesses and countries millions in damages and losses. After all, many managers still hold tightly to the notion that the next dramatic headline about a security catastrophe will be unlikely to feature the name of their organisation.

Instead, what makes these news stories so uncomfortably compelling is that they highlight the open secret in patch management: that almost every successful attack — including Slammer, Nimda, and Code Red — has exploited well-known vulnerabilities that could have been prevented, vulnerabilities for which the software vendors have already issued a software "patch" days, weeks, or even months in advance.

There's one more thing we should note about Slammer: when 15 kilobytes of malicious code is more widely recognised by name than the top three global CIOs, then patch management — together with other critical information security issues — has effectively crash-landed onto the boardroom agenda.

Patch Management Is Now A Critical Business Process

For board members as well as CEOs, CFOs, and CIOs, a patch related problem can contribute to downtime, loss of system performance, credibility issues with customers and business partners, negative public relations, or a compromise to the integrity of user information, intellectual property, or transaction-specific data.

This White Paper:

- Presents the business case supporting an integrated approach to enterprise patch management from an information security perspective;
- Examines the business factors that drive the need for effective patch management;
- Looks at the financial impacts on an organisation when patches are not applied; and
- Outlines the basic architecture that needs to support any world-class approach to patch management — not just as a targeted initiative but also as an integrated component of a fully comprehensive approach to threat and vulnerability management.

Download this White Paper now.

Have a question about this White Paper?

To learn more about PricewaterhouseCoopers' Patch Management solutions, please contact: Jim Barrett, 414.212.1637, or Andrew Toner, 646.471.8327.

The business case support Web services certainly hits the right notes — automation will reduce human error; costs will decline precipitously; efficiency will accelerate.

Enticing but Dangerous: Assessing Web Services From a Data Quality Perspective

By George Marinos, *DM REVIEW™*,
Volume 14, Number 5, May 2004

From boardrooms to IT planning meetings, there is a wave of interest in the promise of Web services. It is a compelling promise: the prospect of leveraging Web technologies in new ways to realize an automated exchange of information in real time and across widely disparate applications.

The business case support Web services certainly hits the right notes — automation will reduce human error; costs will decline precipitously; efficiency will accelerate. Additionally, new service bridges will spring up to link not only business partners, suppliers and customers, but also applications within the enterprise that have never been able to share information. That's a pretty good deal, and it's getting executive attention.

However, woven across the tapestry of benefits is a singular issue with searing consequences for organizations that elect to adopt a Web services initiative without properly understanding its strategic dependency: the quality of the underlying data.

This article also discusses:

- Why executives are concerned about data;
- Why there's a paradigm shift in interoperability;
- Why Web services carry such dangerous implications for data quality;
- What the business and financial consequences are, and
- Why you should look beneath the surface.

Read More

For more information…

George Marinos is PricewaterhouseCoopers' National and Data Quality Partner. He has more than 19 years of experience in the information systems industry, including responsibilities as a developer, systems manager and IT director. He has spent the last six years helping client organizations implement risk management solutions and data quality programs that balance the need for a disciplined approach to people, process and technology challenges with appropriate action along a full spectrum of risks.

Marinos can be reached at george.marinos@us.pwc.com or through www.pwc.com/dataquality.

The combined solution from PricewaterhouseCoopers and PatchLink helps organisations reduce costs associated with a reactive approach to patch management, demonstrate compliance with regulations and industry standards, and reduce or eliminate the negative financial impact of system downtime.

Vendor Alliance Spotlight: PatchLink Corporation

Issues of this newsletter often feature a PricewaterhouseCoopers' strategic Alliance Vendor within one of our practices.

Patchlink Corporation, founded in 1991, is consistently ranked by industry experts as the proven leader of automated security patch management software.

With a strong reputation for providing the IT community with unparalleled network and security management software products, today PatchLink's software is installed on millions of nodes worldwide and with Fortune 500 companies.

Through a strategic alliance with PricewaterhouseCoopers LLP, PatchLink is now helping companies access, strategise and implement an enterprise-wide patch management solution to combat the day-to-day onslaught of system threats and security vulnerabilities. This alliance offers global organisations the ability to enhance their patch management program to integrate patch management technology from PatchLink with industry-specific risk assessment and strategic security planning from PricewaterhouseCoopers.

A combined solution to reduce patch management costs

According to the **"The State of Information Security 2003, Worldwide Study by CIO magazine and PricewaterhouseCoopers,"** global organisations are planning to take a more strategic approach to threat and vulnerability management in 2004.

"An effective patch management program requires a combination of technology, processes and procedures," says Mark Nicolett, Vice President, Gartner, Inc. "Technology alone cannot solve the problem. Companies need to build processes and procedures that clearly define the responsibilities of the various organisational units that are involved in evaluation of a new vulnerability and testing and deployment of a patch or other remedy. The overall process must also include an ongoing monitoring program to stay ahead of new threats and to ensure a sustained focus on vulnerability mitigation."

The combined solution from PricewaterhouseCoopers and PatchLink helps organisations reduce costs associated with a reactive approach to patch management, demonstrate compliance with regulations and industry standards, and reduce or eliminate the negative financial impact of system downtime.

How organisations can benefit from this alliance

Working together, PatchLink and PricewaterhouseCoopers can offer organisations best-of-class solutions and services:

- PATCHLINK UPDATE™ automates the patch management process across a wide variety of operating systems, significantly reducing costs while providing a high level of platform security and availability. Large organisations benefit from features specifically designed to speed deployment, as well as automate monitoring and management across global enterprises.
- PricewaterhouseCoopers' security professionals work with a company's IT team to assess their IT infrastructure and provide a "roadmap" to successfully integrate people, process and technology into a customised patch management solution for the business.

Combining best practices with a multi-platform solution

"Today, regulations and legal requirements have raised the bar on the need for information security," says Andrew Toner, partner, Technology practice, PricewaterhouseCoopers. "Senior executives understand the relationship between sound system security and the integrity of their financial statements and operational reports. They understand the financial and brand impact of system downtime. Proven automated patch management systems that work across multiple and diverse environments are critical in today's extended enterprise.

(see next page)

"Combining PricewaterhouseCoopers' security best practices and industry-specific approach with PatchLink's multi-platform PATCHLINK UPDATE enables our mutual customers to create an integrated, holistic patch management program to enable the 'always on' organisation."

PatchLink's patch management system addresses the issues of a real world enterprise, such as the ability to manage completely isolated network segments commonly found in financial institutions and governmental departments. PATCHLINK UPDATE can be configured to address this enterprise issue. It can also help with additional solutions such as end-point security management, centralised roll-up reporting, and customised configuration management, among others.

"It's critical that a patch management system be able to address all the different types of operating systems in an enterprise from one console," said PatchLink CEO Sean Moshir. "A major focus of our alliance with PricewaterhouseCoopers is to deliver customised solutions supported by a national team of security integrators and patch management professionals. The level of analysis, verification, testing and validation that occurs through our combined offering is an important step forward to improving the speed and success of patch installation within the enterprise."

Want to find out more?

To learn more about security strategy and the integrated patch management solution from PatchLink and PricewaterhouseCoopers, visit www.patchlink.com, or read about the Patch Management Accelerator from PricewaterhouseCoopers — which can help organisations quickly understand how to build a standardised, sustainable patch management solution that integrates people, process and technology.

New Publications from PricewaterhouseCoopers

The Discipline of Enterprise Patch Management — A Critical Component of A Broader Approach to Protection: A White Paper

For board members as well as CEOs, CFOs, and CIOs, a patch related problem can contribute to downtime, loss of system performance, credibility issues with customers and business partners, negative public relations, or a compromise to the integrity of user information, intellectual property, or transaction-specific data. Download

Unlocking the Value of Protection: The Strategic Role of Security Information Management in Accelerating Enterprise Transition to a Proactive Security Posture — A White Paper

Today, there's a critical bottleneck in protection. The absence of critical integration capabilities is raising risk profiles, straining budgets, and threatening performance. Executives today are not only poorly served by their current product-based security infrastructure, but are also unable to command the end-to-end solution required by their threat environment, vulnerability profiles and strategic business objectives. While IT staffs strain to extract value from the vast streams of data, CEOs and CIOs at the corporate helm are having difficulty addressing strategic business issues relating to security.

Unlocking the value of protection begins with a comprehensive approach. The critical step that enables this harvest of value is a strategic commitment to building proactive capabilities in security information management that support the organisation's ability to convert data into information – and information into action. Download

(see next page)

Don't miss these important security events.

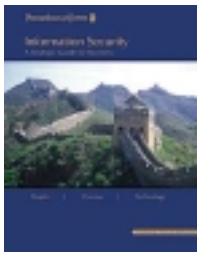
"Information Security: A Strategic Guide for Business"

A new book, part of the PricewaterhouseCoopers' Technology and Risk Management Forecast series, offers organisations a new methodology for integrating highly effective security management techniques into everyday business processes.

Order the Book

This book can be purchased for US$49 (or US$25 by PwC employees) 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.

Managing IT As A Business: A Survival Guide for CEOs



How do you link IT to corporate strategy and manage your IT business risks? How do you recognise the importance of technology as a means of improving customer service? How do you work more efficiently to leverage IT strategically? And how to use it as a driver of business success?

This new book by Mark D. Lutchen, lead partner for PricewaterhouseCoopers' IT Business Risk Management practice, provides a clear framework and reveals practical insights into the most common enterprise IT problems.

Order the Book

Mark Your Calendars! Upcoming Conferences, Seminars and Webinars

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

CONFERENCES

Burton Group Catalyst Conference North America: Evolving Enterprise Infrastructure — Networks, Security, Identity Management, Application Platforms

Date:	July 21-23, 2004
Location:	San Diego Marriott Hotel & Marina, San Diego, CA
Register online at:	https://secure.meetingexp.com/BurtonGroup/CatalystNA2004/registration.php

Catalyst Conference North America will empower and enable you to build the proper network, identity management, and applications infrastructure.

(see next page)

Join us at these upcoming industry events.

CIO 100 Symposium & Awards Ceremony

Date: August 22-24, 2004
Location: The Broadmoor, Colorado Springs, CO
Register online at: http://www.cio.com/conferences/home.html?ID=4
This year, CIO magazine has selected 100 companies that exemplify the leadership and innovation in the use of information technology to increase their organizations' agility. They will bring together this year's winners — along with key business thought leaders to explore how to achieve organizational agility and use it to your advantage in an environment where the only constants are change and uncertainty.

IDC Security and Business Continuity Forum

Date: September 20, 2004
Location: New York, NY
Register online at: http://www.idc.com/getdoc.jsp?containerId=IDC_P8422&selEventType=CONFERENCE
PricewaterhouseCoopers is a diamond sponsor of this event designed to help enterprise decision-makers answer key questions about security and business continuity they are struggling with today — all investigating the next frontiers to secure.

CIO 05: The Year Ahead

Date: November 7-9, 2004
Location: The Fairmont Scottsdale Princess, Scottsdale, Arizona
Register online at: http://www2.cio.com/conferences/november2004/index.cfm
CIO|05: The Year Ahead takes the first look at the likely impact of the results on global affairs, the economy, business and technology. The nation's leading CIOs and senior IT executives explore and discuss the trends and issues we expect to have significant impact on the CIO role in the next 12-24 months, and share ideas on how to derive the most value from IT to help keep the business competitive.

ARCHIVED WEBCASTS

PricewaterhouseCoopers Presents: Spring IT Advisory Web Series — Aligning IT to Manage Risk and Improve Business Performance

Original Broadcast Date: Wednesday, May 5, 2004

Live Video Webcast: Building IT Resiliency – IT's Role in Managing Risk

Original Broadcast Date: Thursday, May 20, 2004

The Journey to World Class Information Security – Starts with a Road Map

Original Broadcast: Wednesday, June 2, 2004

The "Always On" Organisation: Best Practices for Threat and Vulnerability Management

Original Broadcast: Wednesday, June 23, 2004

Managing Digital Identities: How Identity Management Solutions Can Improve Your Business Results

Data Quality: An Essential Building Block to Successful ERP Implementations

Original Broadcast Date: May 19

SAP and PricewaterhouseCoopers LLP Present: The Corporate Governance, Risk, and Compliance Web Series

PricewaterhouseCoopers and SAP have teamed to host the Corporate Governance, Risk, and Compliance Web series to help you leverage your current SAP environment

(see next page)

View our past webcasts.

to enhance your risk management processes. Each session will address specific risk management issues confronting companies today. Representatives of PricewaterhouseCoopers and SAP will share strategies, techniques and tools you can use to improve performance while proactively managing the costs of compliance.

Initial Webcast: Tuesday, March 16, 2004

Gaining Financial Integrity through Improved Internal Controls

Initial Webcast: Tuesday, March 30, 2004

Moving Beyond Sarbanes-Oxley – Focus on Corporate Governance, Risk, and Compliance

Initial Webcast: Tuesday, April 13, 2004

"It's All About Fast" — Accelerated SEC Reporting Requirements

Initial Webcast: Tuesday, April 20, 2004

International Corporate Governance

Data Quality: At the Core of Regulatory Compliance Initiatives

Initial Webcast: April 14, 2004
Duration: 1 hour
View today at: http://www.firstlogic.com/041404.
Featured Speakers:

- Dan DiFilippo, Natl. Lead Partner, PwC Governance, Risk & Compliance practice
- George Marinos, Natl. Lead Partner, PwC Data Quality practice
- Steve Varsolona, Market Development Director, Firstlogic

Sarbanes-Oxley, HIPAA, GLBA, the Patriot Act… and the list goes on. Organisations today must navigate a proliferation of new standards and stakeholder expectations. Many have responded to each in turn, adding another level or type of control and managing the enterprise's response regulation by regulation. For many this approach has become complex, expensive and prone to failure.

Web Seminar: Best Practices in Data Quality

Initial Webcast: February 25, 2004
Duration: 1 hour
View today at: http://www.firstlogic.com/bestpractices_pwc
Join PricewaterhouseCoopers LLP (PwC) and Firstlogic, Inc. as they kick off their iStrategy Web seminar series with featured speaker Ted Friedman, principal analyst with Gartner, Inc'.s Business Intelligence Infrastructure team. As part of the round table discussion, Mr. Friedman will be exploring questions like….Who's accountable for the quality of your data? How are new regulatory requirements affecting the way you manage your data? Can profiling really help you identify data quality issues? Joining Friedman will be James Ruan, Practice Manager for PwC, and Firstlogic's Frank Dravis, Vice President of Information Quality, in this interactive panel discussion covering data quality and management best practices.

Sarbanes-Oxley: How Can I Ensure True Success? A Special META Group and PricewaterhouseCoopers How-To Webcast

Initial Webcast: 13 January 2004
View today at: www.metagroup.com/htwc011304
Or call META at: 1-800-945-6382.
For more information: Contact Sue McKittrick, +1 240 497 0858.
Please join META Group analyst Stan Lepeak along with PricewaterhouseCoopers' Randy O'Hare, partner and chair of the Firm's Sarbanes-Oxley Task Force, for an interactive Webcast addressing SOX needs and highlighting success stories. This session will review Sarbanes-Oxley best-practice compliance processes and supporting IT applications and infrastructure — with an emphasis on longer-term SOX strategic requirements and opportunities.

(see next page)

View our past webinars.

ARCHIVED SECURITY WEBINARS

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

Presented by: PricewaterhouseCoopers and Symantec
URL for viewing: http://enterprisesecurity.symantec.com/content/webcastinfo.cfm?webcastid=73

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"

Initial Webcast: Part One - March 20, 2003
Initial Webcast: 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

Initial Webcast: September 18, 2003
URL for viewing: http://members.netegrity.com/Event.cfm?Id=473&campaction=60

Microsoft Executive Circle Presents: Identity Management in the HealthCare Industry

Initial Webcast: 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

Initial Webcast: 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

Initial Webcast: 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

Initial Webcast: June 19, 2003
URL for viewing: www.netegrity.com/events/events.cfm?page=eventsarchived

WANT TO KNOW MORE?

Please contact Bryan Welch, 415.498.7991.