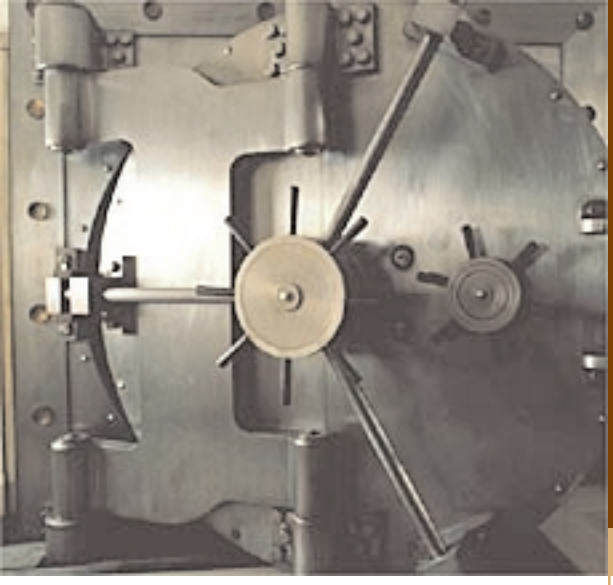


PRICEWATERHOUSECOOPERS

The Secure Solution

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

VOLUME 9, OCTOBER 2002

In This Issue:

This is the ninth issue of The Secure Solution, a monthly newsletter from the Security & Privacy Solutions Practice of PricewaterhouseCoopers. This edition includes a retrospective of cyber security one year after 9/11, best practices for large-scale security implementations, an overview and case study of Enterprise Application and Control Services, a spotlight on a joint product developed by two alliance vendors, and upcoming events covering global 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's global solutions, please contact one of our marketing professionals listed below.

Who To Contact:

James F. Kelly
Americas Marketing Leader
Global Risk Management Solutions
PricewaterhouseCoopers
415-498-5376
james.f.kelly@us.pwcglobal.com

Kate Oliver
Security and Privacy Practice Marketing Director
PricewaterhouseCoopers
860-241-7333
kathryn.oliver@us.pwcglobal.com

And the winner is…

Anne Leary, UNIX System Administrator of Bridgestone/Firestone, is the winner of a Mintek Portable DVD Player, compliments of PricewaterhouseCoopers.

One Year Later: The Cyber Security Implications of September 11th

Jay Ehrenreich, Senior Manager, PricewaterhouseCoopers' Cybercrime Prevention and Response Practice, originally wrote: "The Cyber Security Implications of September 11st" for CPR Newsbytes, November 2001. We recently interviewed Jay for his response to what has changed over the past year, and how these changes affect us all.

Since 9/11/01, there has been a quantum shift in corporate thinking about cyber security.

People in global organizations are more aware of the threat of physical attacks. They now know the degree of damage that can be inflicted to their offices and their computer networks.

At the highest levels, the U.S. federal and state governments are looking at security with heightened senses of reality. Both governments and corporations — all with a heavy reliance on technology — must make security more integral to their business strategies. To be truly safe, physical security precautions must be fully implemented with cyber security measures.

The growing threat

Though the threat of cyberterrorism remains real, few companies have responded to safeguard their computing systems from hackers and intruders. Computer security has always been "the 11th item on a 10-item list," says Harris Miller, president of the Information Technology Association of America.

Furthermore, a summer 2002 poll published by the Business Software Alliance found that 60% of those directly responsible for their companies' network security believe that U.S. businesses are at risk for a major attack on their computer networks within the next year.

Legislation is combating terrorism, ensuring privacy

Over the past year, there has been a tremendous amount of activity in the courts to fight terrorism, boost cybersecurity, and ensure individual privacy:

- The **USA Patriot Act** is setting out measures to combat terrorism. Among other areas, it's developing and supporting cybersecurity forensic capabilities;
- The **National Strategy for Homeland Security** is establishing a foundation to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur;

(see next page)

To be truly safe, physical security precautions must be fully implemented with cyber security measures.

- **Ongoing legislation in Congress** is impacting state governments, such as the decision by North Dakotans in June 2002 to overwhelmingly chose to make banks and credit unions obtain opt-in consent before sharing consumers' financial information;
- The **National Strategy to Secure Cyberspace** — released on 9/18/02 — is providing a road map of what Government (at all levels), Congress, industry sectors, higher education and NGOs (non government organizations) can do as part of our collective national effort to secure cyberspace by preventing viruses and hacker attacks;
- The **Cybersecurity Corps.**, part of President Bush's fiscal 2003 budget, would pay the university tuition of students who agree to do an as-yet-undetermined number of years of government cybercrime work after graduation;
- **BITS**, the Technology Group for the Financial Services Roundtable, was formed by the CEOs of the largest bank-holding institutions in the US as the strategic "brain trust" for the financial services industry in the e-commerce arena to identify issues, develop strategic recommendations, and implement the CEOs' decisions;
- **Cybersecurity Insurance** is an evolving form of coverage being recommended for companies by the Bush administration. Some proponents believe this insurance will be instrumental in steeling the nation's information technology infrastructure against attack.

An international interview on RAI-TV about cyberterrorism

Jay Ehrenreich of PricewaterhouseCoopers was interviewed on July 19, 2002, on the "Planet Economy" program on RAI-TV in Rome, Italy. This International Herald Tribune segment was broadcast in 90 countries throughout Europe, the Middle East, Asia, and on more than a dozen airlines. Here is an excerpt from that transcript…

Anchor: …Most people think that upgrading their systems is enough to solve the problem, but the hackers are still there. What could a government or a company do to rid themselves of hackers?

Mr, Ehrenreich: …There is a circle of technical people who identify the software problems and they develop security measures and then the distributors try to correct these situations with the so-called patch. It's like a race between the hacker and the ones to do the patch. Who can get there first? In this way, the companies have to always be on their toes and have to implement this patch as soon as possible.

Anchor: …Often we hear about Al Qaeda's network and its capabilities. But in reality there's an entire sector; an industry whose main objective is a cyberspace attack. Do you think it's that easy to hire freelancers or mercenaries to train them to hack? It is really difficult to find help for those who are planning to attack to find help?

Mr. Ehrenreich: This is certainly true. There are standard training programs for security consultants to teach them how to attack. And they are readily available. If we go to amazon.com and we look for books about hacking, pirating, we'll find a lot of them. There's a ton of information. And yes, in a few cases one can turn to foreign countries to hire these technical experts who could attack. You see that there is a lot of ready information. And then there are attacks that after the initial blow are applauded by fans or rather they are made easier with the appropriate tools.

Anchor: A cyber-attack is one thing, but the greater fear is a combination, or better yet, the attack on the Web and an attack on humans or other targets such as an attack on the financial market, on the banking system and even worse, on a nuclear facility. Would this be the greatest danger?

Mr. Ehrenreich: I think that… a cyber attack combined with a physical attack… would be the worst case scenario. Since a lot of damage can be done with a cyber

(see next page)

"The real threats to any company's cybersecurity are former employees or consultants who've been fired…"

— Jay Ehrenreich, Senior Manager, Cybercrime Prevention & Response Practice, PricewaterhouseCoopers

attack, for instance by destroying the networks, destroying and stealing data, and of course if all this is combined with a physical attack, the whole thing can become very serious. This could have an impact associating it with a physical attack. It would mean that the whole thing would have to be redone and it would have very serious repercussions…

Don't forget the six golden rules of cybersecurity measures

In his original article last November in CPR Newsbytes, Mr. Ehrenreich listed these six "appropriate" cybersecurity measures that businesses and government agencies should be taking. These golden rules remain the same:

1) Threat and vulnerability assessments should be updated regularly.
2) Information about threats and vulnerabilities should be shared.
3) Effective security policies and procedures should be implemented.
4) Computer security should be re-assessed and upgraded continually.
5) 7x24 monitoring, including intrusion detection systems, should be deployed.
6) Security incident response plans should be developed, and coordinated with overall contingency plans.

Conclusion

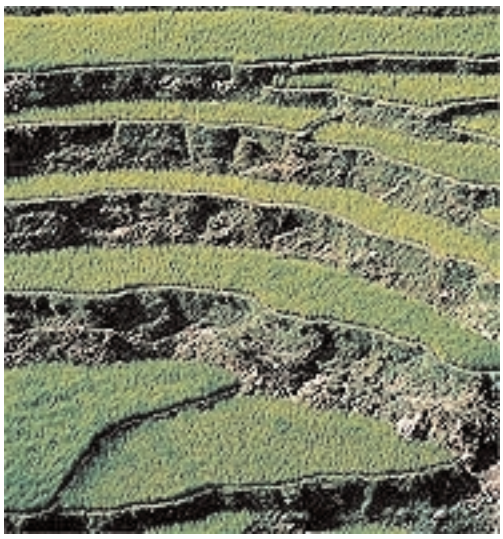
Organizations can greatly improve the cybersecurity aspects of critical infrastructure protection. The question of how much money needs to be spent and how much effort is required will be different for each organization because each one has a different risk/cost/benefit profile.

PricewaterhouseCoopers has vast experience in responding to and investigating cyber crime incidents for our corporate clients. While highly motivated highly technical attacks are very difficult to stop, we know that risks can be minimized, and the impact of attacks blunted, through careful preparation.

The vast majority of incidents we respond to could have been easily prevented had basic security measures been in place, an objective achievable at relatively low cost.

For more information…

To maximize cybersecurity for your company and minimize the threat of cyberterrorism, please contact Jay Ehrenreich, jay.enrenreich@us.pwcglobal.com, 646.471.8018.



"Research and experiences show that most of the problems with the IT implementation don't stem from the technology itself, but rather from all the organizational issues surrounding a large-scale project."

— Mike Peterson, Manager, Project Advisory Services, PricewaterhouseCoopers

Thinking Big: The Main Steps for Large-Scale Security Implementations

Security projects are implemented to achieve specific business benefits. These benefits can include improving vendor management through a new Web portal, enhancing customer service through more robust 24/7 access to account information that simultaneously decreases the need for customer service staff, or providing a single directory containing information for all users across an organization.

As with any IT implementation, these projects are fraught with risks. Worst case implementation for large-scale projects won't yield the anticipated benefits.

"Research and experience show that most of the problems with IT implementations don't stem from the technology itself, but rather from all the organizational issues surrounding a large-scale project," says Mike Peterson, Manager, Project Advisory Services, PricewaterhouseCoopers. "These include securing funding, gaining and maintaining executive level support, and dedicating skilled people to staff the project throughout its full life cycle. Other problems relate to ensuring the organization can exploit the new technology system once it is ready to go live."

The factors that put an IT project at risk, especially an innovative project such as a security implementation, can be controlled through effective project management techniques and methodologies. These techniques increase the likelihood of a successful IT project implementation — employing technology that the organization can actually use to achieve real business objectives.

Key security implementation project risks

1) Organizational change management — "This is the most important risk that must be managed to ensure the organization realizes the benefits of the project," notes Peterson. "This a particularly challenging issue when implementing a new technology in a new way to the organization."

For example, with a security project that will enable new and valuable security strategies in the organization, the company should:

- Specifically dedicate one workstream to defining a new security policy;
- Also dedicate a second workstream to communicating the new policy and security strategy to employees to ensure the whole organization is prepared to take advantage of the available benefits.

The communication policy should enable employees to understand that the security project is not just about new passwords, but doing business better — and that there are benefits for the whole organization in supporting that new technology.

2) Sponsorship/Ownership — "Who is going to support the project at an executive level and have accountability for it?" adds Peterson. "In security implementations, this can be complicated because the sponsor is usually someone within the IT organization, but the "owners" of applications being integrated into the security infrastructure, and ultimately the owners of the business value, are individual business unit managers. To be successful, the project team needs support from both groups."

Important factors include:

- Sponsors and business owners should be clearly identified during project initiation;
- A control process must be in place to ensure the sponsor remains in the loop.

Controls can include presenting regular updates to sponsors and owners, including them in the escalation process for resolving issues, and requiring formal sign-off of deliverables at key points in the project.

(see next page)

The factors that put an IT project at risk… can be controlled through effective project management techniques and methodologies.

3) Scope management — "This is an issue that absolutely must be managed throughout the project," continues Peterson. " Scope refers to the work required to deliver a product with the specified features and function. In a security implementation, "scope creep" is a particular challenge because the technology is so new that it is difficult to have a complete understanding at the beginning of the project of the amount of work required to complete it."

Scope changes can also be caused by the need to expand the projects to include more business units. The key to controlling this risk is a strong scope management process, including:

- Scope planning;
- Scope definition;
- Scope verification; and
- Scope change control.

It's critical that scope change control requires appropriate review and sign-off of any scope changes *before doing work*.

4) Funding — "Depending on the IT organizational model in use," says Peterson, "funding for a new security infrastructure and integrating applications into the infrastructure can be complicated. Existing security budgets are not likely to be large enough to;
A) Support building a new security infrastructure, and
B) Integrating the applications from all interested business units. Rolling out new security solutions can require a new funding model that will allow business units to budget and pay for integrating applications into a new security architecture."

The keys to controlling this risk are:

- Proper up-front planning and building in controls for regular review of budget and scope;
- Ensuring that funding is in line with current and future project and business needs.

5) Resources — "Most organizations don't currently have staff with the skill sets required to implement many of the cutting edge security solutions, nor are these individuals readily available to hire," adds Peterson. "Nor do organizations have adequate staff on hand to support the technology long term."

Again, the key to controlling this risk is good planning up front. Planning should also include:

- A short-term strategy to partner with an implementer to provide needed skills; and
- A strategy to acquire the skill sets necessary to support the technology long-term.

6) Issue and risk management — "Managing risks and issues are more difficult on security projects because the projects span organizational boundaries," concludes Peterson. "Some issues will affect IT process, while others will affect individual business units and associated processes."

The key to controlling this risk is to create a process for identifying, reviewing, escalating and resolving management issues at the appropriate level, in the appropriate organization.

The impact of not controlling risks

By carefully controlling project risk, you can meet business objectives for a large-scale security implementation. However, if any or several of these risks are not properly managed, you can experience problems that will have significant impact.

(see next page)

"We're now bringing the benefit of added value to our clients with e-business based portal products, including application security and control services."

— Mike Stough, Americas Partner In-Charge, EACS, PricewaterhouseCoopers

Failing to meet objectives can result in a delayed product launch date, which negatively affects customer satisfaction; a less-than-desired implementation of the levels of security, resulting in a security infrastructure that is vulnerable to abuse; or a dissatisfied business who may not wish to consider future projects.

Take the next step

To learn more about how to deploy large-scale security implementations, contact Mike Peterson, Manager, Project Advisory Services, PricewaterhouseCoopers, michael.peterson@us.pwcglobal.com, 313.394.6924.

Portal Play: The Evolution of Enterprise Application & Control Services

Sometimes, change is good. For Enterprise Application and Control Services (EACS), what has worked in the past is now evolving to what may work better in the future.

"For seven years, our experts have put security at every point of entry by collaborating with our Business Process, Controls & Security, and Change Management teams," says Mike Stough, PricewaterhouseCoopers' Americas Partner In-Charge, EACS. "Our suite of services has supported each clients' workforce productivity and back-office controls. But as more clients implement portal technology to enable their users with greater Web access, they're looking at applications outside of their main Enterprise Resource Planning (ERP) systems."

To date, many EACS engagements have been with large-scale ERP applications that are now being upgraded to support Web-based access and transaction processing. In addition, many smaller applications are being redeveloped using newer Web-based application products, such as Microsoft® .NET or IBM's WebSphere®. These, too, need to be secured and controlled.

Bringing added value to our clients

"Our future looks very exciting," continues Stough. "After a solid financial year in 2001 with on-going engagements from both existing and new clients, we're now bringing added value to our clients' Web-based portal initiatives by implementing application security and controls."

"Many companies may not yet realize that they do not have the proper security controls in place," notes Stough. "They should consider a review by a security expert to access their needs and implement the right controls for their business before they deploy these new portal products."

Design and implementation of a secure portal

A new portal product is being rolled out worldwide with a current engagement. "My client is a major pharmaceutical company," says Ying Zhou, EACS Manager, PricewaterhouseCoopers. "The challenges we're facing are staggering. To design and implement a secure portal strategy to its employees and user community, there are numerous barriers."

These include:

- Seamlessly integrating a global decentralized operation with disparate operating company practices into one centralized Intranet;
- Bringing thousands of employees and third-party contractors throughout the US and Europe together onto one system;

(see next page)

Within EACS, PricewaterhouseCoopers offers four key services that apply to enterprise initiatives:

- *Application security services;*
- *Workforce productivity and back-office control services;*
- *Supply Chain Management (SCM) control services; and*
- *Customer Relationship Management (CRM) control services.*

- Ensuring security with consistent user restrictions across the various systems; and
- Enhancing the user experience.

PricewaterhouseCoopers is succeeding by:

- Utilizing SAP's Central User Administration technology — User data is being stored and updated from multiple source systems into one central system via user synchronization;
- Using Role-Based Access Control (RBAC) methodology in security role design — Without sacrificing portal presentation needs, we're reducing maintenance costs and ensuring flexibility;
- Designing and assigning user access from each of the source systems — Access is automatically mapped in the portal, facilitating segregation of duties analysis.

"All the user creation and updates happen only once in the central system," says Ms. Zhou. "This substantially reduces the user maintenance needs in different systems, including the portal."

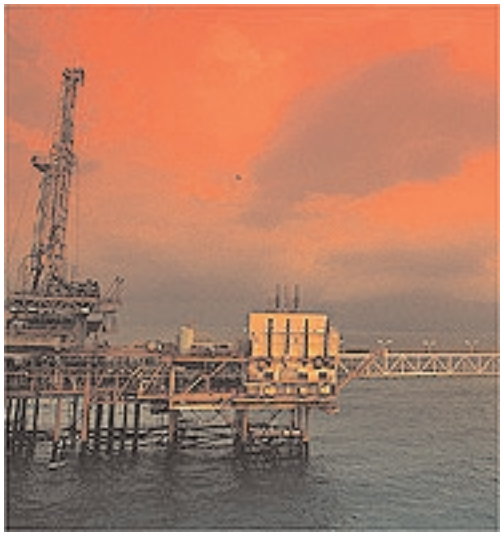
Tools and technologies can speed implementation

PricewaterhouseCoopers has developed an array of tools and technologies to leverage our practitioners' experience and help expedite application control projects. Many more tools are available, but the main ones include:

- **Risk Management Dynamo –** Supporting the work of our SAP implementation specialists, this tool allows a project team to build the appropriate control structure needed for any implementation, leveraging our robust database of risks and controls. Contained in this extensive library are risks that should be considered in every SAP implementation, as well as configuration tasks and review procedures.
- **Automated Controls Evaluator (ACE) –** A sophisticated SAP interrogation tool, ACE helps our professionals evaluate segregation-of-duties conflicts and other risks within an organization's SAP application. Using samples of client data and this proprietary database tool, our specialists can fully analyze SAP security.
- **PricewaterhouseCoopers SAP Security and Control Accelerators —** An extensive repository of innovative tools, proven accelerators and best practices, to which our global practitioners contribute regularly. Using samples of client data is one way in which PricewaterhouseCoopers proactively manages its intellectual property and shares lessons learned.

Learn more

For more information on the PricewaterhouseCoopers comprehensive Enterprise Application and Controls Services, please read the EACS Case Study, or contact Mike Stough, michael.d.stough@us.pwcglobal.com, 804.697.1711.



"The client was able to implement SAP quickly and effectively. They estimate they'll save $267 million in operational improvements, procurement and administrative efficiencies over five years."

— Mike Stough, Americas Partner In-Charge, EACS, PricewaterhouseCoopers

Enterprise Application & Control Services Case Study: What We Did For A Global Energy Company

This newsletter will frequently profile a PricewaterhouseCoopers Security & Privacy solution and client engagement. Because of the extremely sensitive nature of our customers' security issues, we can reveal their industry, but not their company's names. All facts, results and benefits detailed here are actual.

Description of Client's Business

The company is engaged in worldwide exploration and production of crude oil and natural gas, domestic refining, marketing and transportation of petroleum products and other energy-related businesses.

The Client's Challenge

"The client had undertaken an implementation of SAP (r/3 4.6c)," says Mike Stough, Americas Partner In-Charge, Enterprise Application & Control Services, PricewaterhouseCoopers. "The timeline was extremely aggressive because they sought to improve profitability by year's end. With the tight timeframe, they were concerned that security and controls would not be given enough focus."

This client needed:

- Experienced resources to quickly start work in both the security and business process control areas; and
- A comprehensive SAP security strategy that would complement their current IT strategies.

The PricewaterhouseCoopers Solution

"PricewaterhouseCoopers took a risk-based approach to targeting the business processes to focus on in identifying controls and security requirements," continues Stough. After the high-risk processes were identified based upon the client's business environment, the controls team:

- Utilized Risk Dynamo, PricewaterhouseCoopers' proprietary tool, to expedite the identification and documentation of necessary control;
- Identified the appropriate segregation of duties that needed to be in place; and
- Provided this information to our security development team.

The security development team set out to determine methods to expedite the identification and development of roles. Some of the tools and accelerators used included:

- Creating custom databases for documenting roles and assigning users;
- Developing Computer Assisted Testing Techniques scripts (CATTS);
- Integrating databases with the training team and the organizational design team to leverage each team's data; and
- Deploying Risk Dynamo, containing best practices for SAP controls work.

We also worked as a liaison between the project team and the client's Internal Audit group. Through this, we assisted Internal Audit in gaining an understanding of how security and controls were being addressed.

Benefits/Results to the Client

"The client was able to implement SAP quickly and effectively," says Stough. "In fact, they estimate they'll save $267 million in operational improvements, procurement

(see next page)

Oblix·IDLink for BMC

"This integration with BMC Software provides customers the ability to deploy an end-to-end identity management solution that will scale with their growing business."

— Gordon Eubanks, President & CEO, Oblix

and administrative efficiencies over five years." For them, SAP:

- Provides a foundation for greater collaboration and partnering within the industry;
- Enables the use of balanced score cards;
- Provides e-business processes;
- Improves information flow: data is entered once, information is more accurate and sharable; and
- Implements business practices based on best practices.

"The PricewaterhouseCoopers work enabled the SAP implementation to be completed to ensure that security and controls were not sacrificed at the expense of the aggressive timeline," adds Stough.

Contact Us

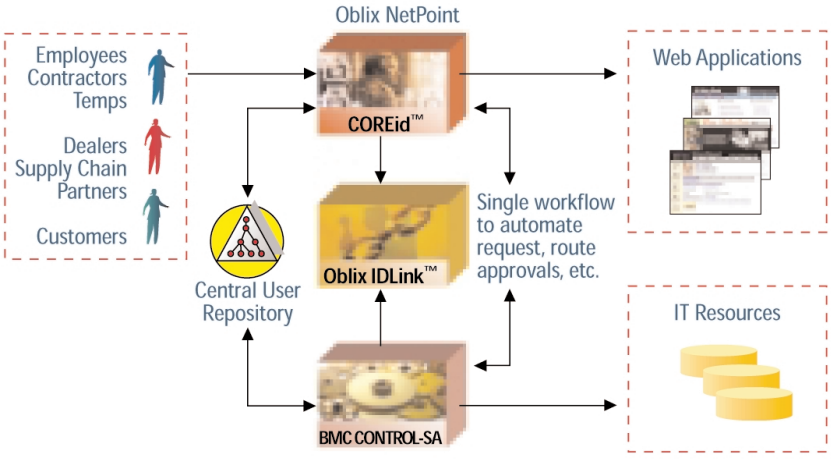
To find out more about PricewaterhouseCoopers' Enterprise Application & Control Services, please contact Mike Stough, michael.d.stough@us.pwcglobal.com, 804.697.1711.

PricewaterhouseCoopers Alliance Spotlight: Oblix and BMC Software Introduce IDLink to Provide End-to-End Identity Management

Each issue of this newsletter will feature a PricewaterhouseCoopers' strategic Alliance Vendor within our Security & Privacy Practice.

Oblix (www.oblix.com), a leading provider of identity-based security solutions and BMC Software, Inc.(www.bmc.com, NYSE: BMC), the leader in enterprise management, recently announced a new product called Oblix IDLink™.

The product, which was developed by Oblix in cooperation with BMC Software, facilitates end-to-end identity utilization between Oblix NetPoint and CONTROL-SA® by BMC Software. By combining these two best-of-breed solutions, enterprise customers now have one Web-based system for managing all user information across their entire Web and IT environments.



Packaged solution linking together real-time enterprise identity management and provisioning back-end IT resources.

(see next page)

"We're integrating Oblix NetPoint to provide COREid, an identity infrastructure which serves as the foundation for an entire e-business environment."

— Steve Lesem, Vice President, Security Business Unit, BMC Software

Initial interest is running high with Oblix customers

"The jointly developed IDLink shipped on August 30 and is priced at $50,000 per server," says Ann Nash, Director of Marketing for Oblix. "Specifically, this integration enables a single management infrastructure to provide access control, manage digital identity information and provision both internal and external users for all Web-based applications and back-end heterogeneous IT resources. Over 30 customers are currently evaluating IDLink for their end-to-end identity management needs."

"We hit the ground running with this product offering, so we're seeing tremendous momentum," adds Nash. "Customers crossing all industry segments who are deploying large scale extranets are coming to us with the need for this solution. Just some of the customers currently evaluating IDLink include leading North American financial institutions, a national department store, a prominent healthcare company, energy and utilities companies, technology corporations, a transportation leader, and more. We've also briefed and shown a demo of IDLink to the industry analyst community and they confirmed this solution solves a critical customer need and is an industry first."

Joint customers are benefiting at BMC Software

"We're integrating Oblix NetPoint to provide COREid, an identity infrastructure which serves as the foundation for an entire e-business environment, with CONTROL-SA enterprise user provisioning," says Steve Lesem, Vice President, Security Business Unit, BMC Software. "So we're able to give our joint customers a comprehensive identity management solution that delivers increased manageability and decreased costs. This integration allows us to extend our provisioning capability into the Web environment and provides customers the ability to streamline their processes for granting access to any enterprise application."

"Over the years, we've seen a lot of marketplace interest," continues Lesem. "But with IDLink, it's faster than usual. There's a lot of grouping in the IT world, but the differentiated alliance of BMC, Oblix and PricewaterhouseCoopers investing time and resources into each other's businesses is definitely shifting the paradigm. One measure is that our customers are very interested. But the real measure is that going into the marketplace with this type of triad is definitely changing things in our competitors' eyes."

"As organizations grow their online businesses, both in terms of people and applications, they need to find ways to cost effectively scale their environments," said Gordon Eubanks, President and CEO, Oblix. "This integration with BMC Software provides customers the ability to deploy an end-to-end identity management solution that will scale with their growing business, no matter how complex the environment becomes. We are pleased to work with BMC and provide this unique solution for our joint customers."

A combined solution for complex IT environments

As enterprise organizations continue to move more business initiatives online, IT environments become more complex. Both internal users (employees, contractors) and external users (customers, partners) need secure access to all types of applications—Web-based, mainframe and client-server.

Typically, managing identities and access rights for provisioning IT resources of users is accomplished using separate consoles, applications and data repositories than those used for managing identities and access rights to Web-based applications and resources. Not only has this required IT departments to duplicate administrative tasks and increase their security risks, but this model for identity management does not cost effectively scale as online business grows and extranet environments become more complex.

Oblix IDLink addresses this problem by:

- Providing the technology that combines the strengths of Oblix NetPoint Web access and enterprise identity management with CONTROL-SA enterprise user provisioning;

(see next page)

"We're seeing a huge need from our clients to have an end-to-end identity management system across their enterprise."

— Joe Duffy, Global Partner-in-Charge, PricewaterhouseCoopers' Security & Privacy Practice

- Using Oblix NetPoint to provide Web single sign-on to any enterprise application; and
- Enabling an identity management infrastructure, COREid™, by BMC Software to fully leverage enterprise-wide access management.

The same user identity information managed by Oblix NetPoint for Web access, now also drives uses CONTROL-SA's user provisioning backbone across multiple back-end heterogeneous IT resources (Microsoft Active Directory, LDAP Servers, UNIX, mainframes, email systems, HR, ERP and many others).

How PricewaterhouseCoopers is linking with IDLink

"We're seeing a huge need from our clients to have an end-to-end identity management system across their enterprise," says Joe Duffy, Global Partner-in-Charge, PricewaterhouseCoopers' Security & Privacy Practice. "The powerful combination of Oblix NetPoint for enterprise identity management and BMC Software CONTROL-SA for processing provides a state-of- the-art enterprise wide identity management system for companies conducting business on the Web."

"PricewaterhouseCoopers is presenting Oblix IDLink to several clients and is receiving a very enthusiastic response on the integrated BMC Software and Oblix solution," says Jerry Lewis, Partner, Security Integration Services, PricewaterhouseCoopers. The majority of these clients have very complex business environments and need an identity management infrastructure that enables them to scale their businesses while also reducing operational costs."

A single end-to-end solution offering multiple features

Specific features of the integrated solution include:

- **Single point of control** through the Oblix NetPoint GUI for managing digital identities and access rights for all users to all applications throughout the extended enterprise;
- **Single process for end-to-end user-set-up, user changes and de-activation of user accounts** in both Web-based and back-end IT resources;
- **Single workflow system with automated requests and approvals** for new users and their access to both Web-based applications and back-end IT resources;
- **Combined role-based (access to applications based on a single attribute) and rule-based (access to applications based on a combination of roles or a specific business rule) provisioning and identity management**, providing maximum flexibility in developing access rights for complex environments;
- **End-to-end self-service and self-registration** through one interface for all applications; and
- **End-to-end delegated administration for provisioning users to IT resources and user identity management** to be distributed throughout the extended enterprise. Not only does Oblix IDLink produce operational cost savings by reducing the duplication of manual tasks, but it also increases security because access can be immediately discontinued to all resources for employees or business associates who are no longer permitted to access those resources.

For more information…

To receive further information, please download the Oblix IDLink Data Sheet at http://www.pwcglobal.com/Extweb/manissue.nsf/docid/0DAD2B3D9CFA129685256C52007E1EEC

At Oblix, contact Ann Nash, Director of Marketing, anash@oblix.com, 408.861.6834.

At BMC Software, contact Steve Lesem, Vice President, Security Business Unit, Steve_Lesem@bmc.com, 713.918.1998.

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 in October and beyond.

CONFERENCES

BMC Software FORUM 2002 Dallas

Date: October 15-16, 2002
Location: Adam's Mark Hotel, Dallas, TX
Register online at: www.bmc.com/forum/dallas/dallas_reg.html
For more information, call 1-800-574-4262

IAPO Privacy & Security Academy & Expo

Sponsored by: International Association of Privacy Officers and PricewaterhouseCoopers
Date: October 16-18, 2002
Location: Chicago Marriott Downtown, Chicago, IL
Register online at: www.gocsi.com/annual/index.html

BMC Software FORUM 2002 San Francisco

Date: October 21-22 2002
Location: San Francisco Marriott, San Francisco, CA
Register online at: www.bmc.com/forum/sf/sf_reg.html
For more information, call 1-800-574-4262

BMC Software FORUM 2002 New York

Date: October 30, 2002
Location: Sheraton New York Hotel & Towers, New York, NY
Register online at: www.bmc.com/forum/ny/ny_reg.html
For more information, call 1-800-574-4262

BMC Software FORUM 2002 Washington

Date: November 6-7, 2002
Location: Hilton McLean Tysons Corner, McLean, VA
Register online at: www.bmc.com/washington/washington_reg.html
For more information, call 1-800-574-4262

CSI 29th Annual Computer Security Conference and Exhibition

Sponsored by: Computer Security Institute
Date: November 10-12, 2002
Location: Hilton Chicago Towers, Chicago, IL
Register online at: www.gocsi.com/annual/index.html

Forbes CIO Forum

Sponsored by: Forbes Magazine
Date: December 9-10, 2002
Location: Four Seasons Resort and Club at Las Colinas, Irving, TX
Register online at: http://www.forbes.com/conf/cio/index.shtml

(see next page)

Join us for these upcoming conferences.

Infosecurity 2002

Sponsored by:	Reed Exhibitions
Date:	Conference: December 10-12; Exhibition: December 11-12, 2002
Location:	Jacob K. Javits Convention Center, New York, NY
Register online at:	http://www.infosecurityevent.com/App/main.cfm?moduleid=42&appname=100004

WANT TO KNOW MORE?

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