UBM TechWeb

darkreading.com

Next

SECURITY dark READING

DECEMBER 2011

Protect The Business Enable Access

Database access controls keep information out of the wrong hands. Limit who sees what to stop leaks—accidental or otherwise. >>

By Debra Donston-Miller

Plus: User provisioning isn't as simple as it sounds >>

Take Aim At Database Access

TIM WILSON

One of the most mundane yet critical functions of a security administrator is to ensure that users have access to all the systems and data they need to do their jobs—and limited or no access to the ones they don't. This so-called "user provisioning" process sounds simple, right? It isn't.

The problem, in a nutshell, is that a "job" is a moving target. Every day, some employees are given new responsibilities while others are left behind. The goals and purposes of the company shift, and whole groups of employees are given new marching orders. Users find that some existing tools are essential to their redefined jobs, while others go completely forgotten.

Think about your job for a moment. How much has it changed since you joined your company or were issued your current computer? How many applications in that original desktop configuration do you actually use? How many new tools, systems, and applications have you gained access to in order to execute some new project or responsibility?

The fact is that user provisioning isn't something you do once and forget. IT organizations must be vigilant not only about giving users access to the data they need for their jobs but also about locking them out of data they no longer need or never used in the first place. It's easy for IT administrators to give users too much access—restricting access is more time-consuming and can create ornery users. Yet, too much access is often what leads to data breaches and leaks that can have enterprise-wide implications.

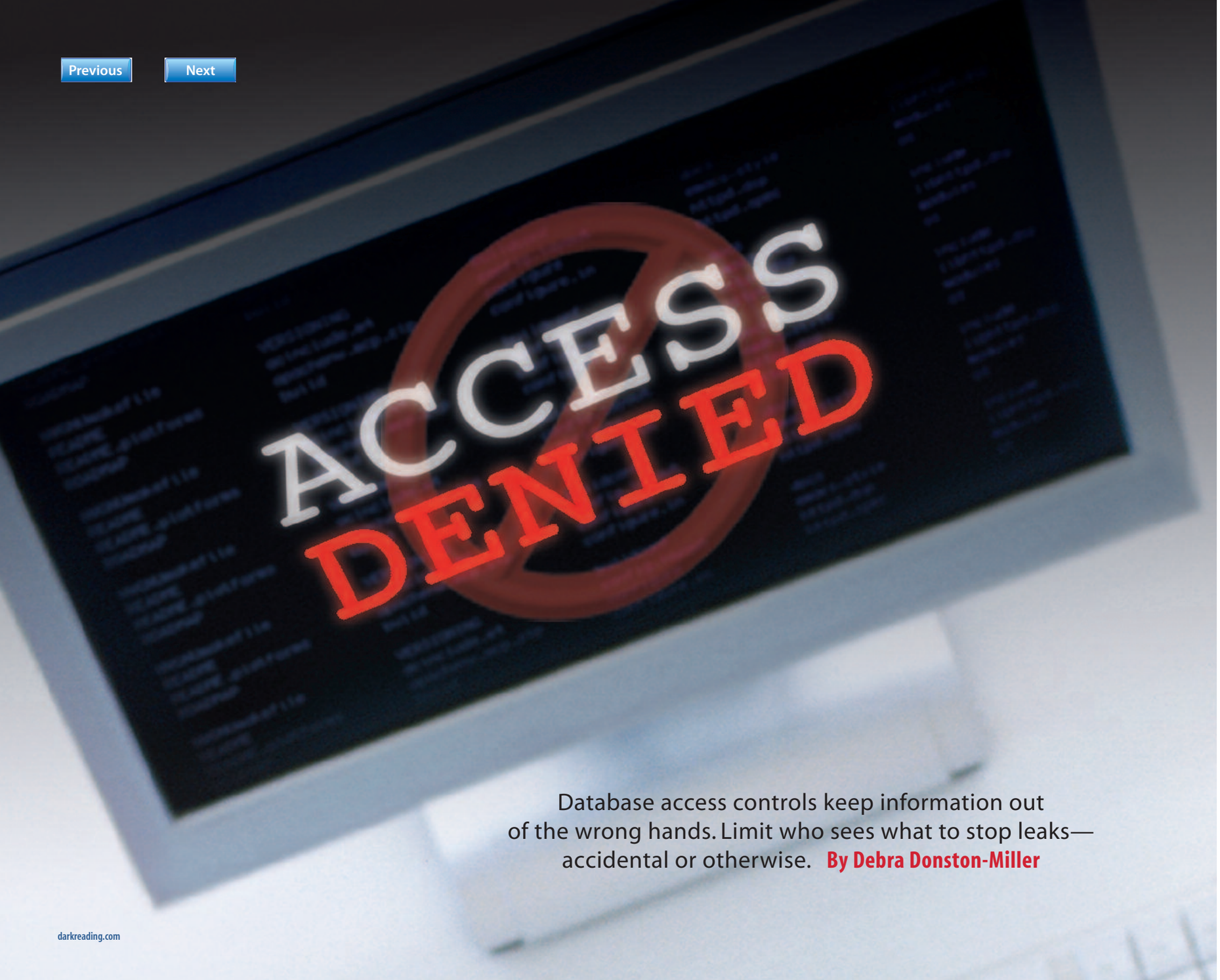
It's easy to give users too much access—restricting access is more time-consuming and can create ornery users.

Nowhere is this problem more evident than in the world of databases, which often contain the company's most important and sensitive information. Controlling who can access customer lists or account information is essential to enterprise security, yet the list of authorized users may change daily as employees come and go, their responsibilities shift, and top executives ask for a peek at this or that data.

In this *Dark Reading* supplement, we examine how to provision database access so that only users who need the information can get into it at any given time. While role-based access control is the basic method for handling this provisioning, there are many ways to tune the administrative process to fit the needs of the user and the company. We provide tips and best practices for doing that tuning.

If you're wondering who has access to your critical database information—and whether they really should have that access—then this supplement is for you. Just remember that the role of the user and the goals of the business are always shifting. Database access provisioning, like many other jobs, is a moving target.

Tim Wilson is editor of DarkReading.com. Write to him at wilson@darkreading.com.



Database access controls keep information out of the wrong hands. Limit who sees what to stop leaks—accidental or otherwise. **By Debra Donston-Miller**

With more data coming from the many new devices and applications in use today, a business' success increasingly hinges on its ability to capture, analyze, manage, and secure data. Companies that nimbly respond to data that their customers and potential customers generate via social media and other sources have a huge advantage over competitors, but that also puts a target on more than just credit card and Social Security numbers. Controlling who gets what level of access to this valuable data is a matter of great complexity and concern. But it's

also vital to ensuring data security.

A company database should be one of the most carefully protected systems in the data center—ideally, the most protected—but all too often this isn't the case. There are various reasons for not making database security a priority. For one, some companies don't know where all their data stores are. This knowledge gap is more prevalent than ever as new types of data are being collected and analyzed. In addition, database systems are notoriously complex, and many companies don't have the expertise to properly secure and monitor database servers. However, businesses that have suffered through a database breach, with the accompanying embarrassment, legal woes, and loss of business and customer trust, would be the first to say that no amount of time and money is too much to spend on database security.

Since 2005, the number of records exposed as a result of data breaches stands at 542,355,248 and counting, according to the Privacy Rights Clearinghouse. External attacks have caused many of the most high-profile database breaches. But a far more insidious threat comes from insiders who have legitimate access to the database but knowingly or unknowingly breach the data.

Not all breaches are malicious. But even the

accidental exposure of, say, healthcare or financial information to an employee who shouldn't have access to it can be a big and potentially costly problem for companies that must comply with regulations such as the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act.

These mandates require minimum standards for information security and, in the case of Sarbanes-Oxley, for role-based access control. "You can't unsee data you have been exposed to, whether you meant to see it or not," as one expert interviewed for this report says.

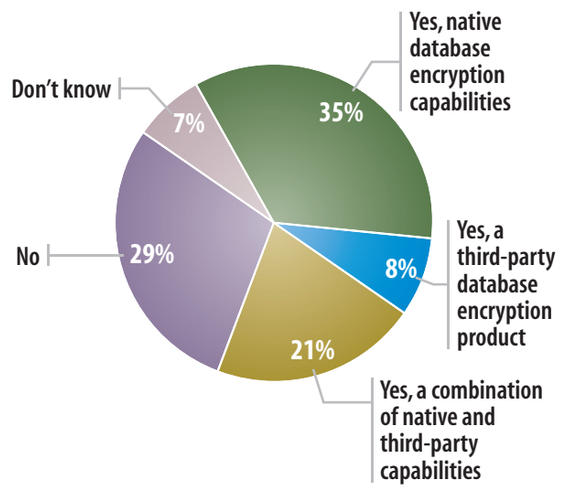
Who, What, Why, And When

There are many security measures that can and should be used to protect a company's database servers. Sixty-four percent of the 755 business technology pros surveyed in *InformationWeek*'s 2010 State of Database Technology Survey said their companies use some form of database encryption, 47% use a database firewall, and 74% use transaction logging on databases containing sensitive information.

While all these protections help safeguard the data, one of the most effective means of ensuring data integrity is user provisioning. It may seem like a no-brainer, but too many companies spend too little time determining who should have access to what data, when they should have this access, and why.

A Sensitive Issue

Does your company use encryption on databases that contain sensitive information?



Data: *InformationWeek* 2010 State of Database Technology Survey of 755 business technology professionals, August 2010

Role-based access control isn't a new approach, but it's still considered the gold standard for provisioning user and application access. With RBAC, access is controlled through roles assigned to users that frequently align with their job functions. Permissions are assigned to roles, and roles are assigned to employees.

"You have to look at this in terms of roles, because that's the easiest way to manage it," says Karen Padir, VP of products and marketing at EnterpriseDB, which provides enterprise-level products, support, and services for the open source PostgreSQL database. It's not a question of whether you're trustworthy, Padir says, but rather it's a question of "what is your job and what do you need to access to go about your job? For example, if your job function is engineer, you should be able to look up in the company database everyone's name and job description or function, but not their salary or their home address, things like that."

Roles range from highly privileged administrators to end users with bare-bone rights. Commercial and open source databases typically come with a set of predefined roles, but these roles tend to be general, so companies should develop ones that make sense to their industry, size, and other specific factors.

That said, companies must strike a balance between ensuring stronger security and easier administrations. As the number and granularity of roles increase, so too does the task

of tracking all those roles and assigning them appropriately.

The Benefits

Role-based access control provides several benefits, according to the "Economic Analysis Of Role-Based Access Control" report prepared by RTI International for the National Institute of Standards and Technology. Among them are the following:

>> Greater visibility of permissions assigned to users and easier verification of internal controls, providing more efficient access control policy maintenance;

>> Reduced costs of administering and monitoring permissions compared with access control lists and other antecedent access control models;

>> Less new employee downtime;

>> Enhanced organizational productivity;

>> Enhanced system security and integrity.

There are other ways of provisioning access—according to identity or the data itself, for instance—but most of these models get complicated fast.

"Managing access based on identities quickly becomes unmanageable after a dozen or so users, which means role-based access is the way to go," says Michael Cobb, founder and managing director of Cobweb Applications, a consultancy that provides data security services, and a Microsoft Certified Database Administrator.

RBAC also lets companies develop and enforce specific requirements for access to certain data, says Cobb, who co-authored the book *IIS Security*. "With roles, you can more easily implement something like 'Role A can access PII data, therefore before anyone can be assigned role A, that person must pass data handling awareness course 2,'" Cobb says.

EnterpriseDB's Padir, who previously was VP of engineering at Red Hat and oversaw identity management and products for single sign-on and user and role provisioning at Sun Microsystems, says, "You have to do it in logical groupings so you don't give yourself a management headache. Individuals change, roles don't."

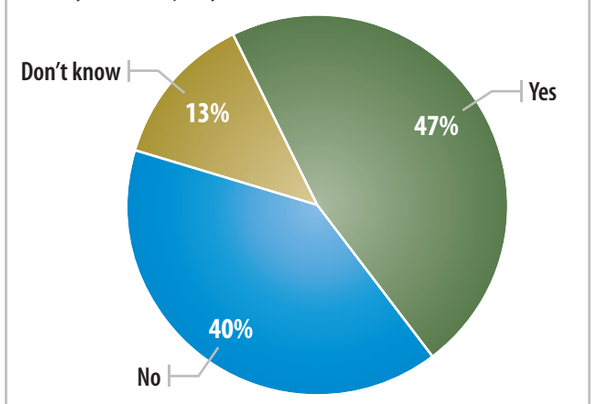
Least User Privilege Still The Way To Go

The types of data companies are collecting and the way they're using that data may be changing, but one database security basic still holds true: Give users access only to the data they need to do their jobs. It's more challenging these days to determine just which users need access to what data, but taking the time to make those decisions is key.

To effectively apply this least privilege model, security professionals need to audit the various roles across the company and, working with business managers, determine what data the people assigned to each role need to do their jobs effectively. This can be a time-consuming process, which is why companies sometimes don't do it—or don't do it well—but the resources invested will pay off.

Weak Defenses

Does your company use a database firewall?



Data: *InformationWeek* 2010 State of Database Technology Survey of 755 business technology professionals, August 2010

For one thing, once the initial work is done, it's done, and the data needs only to be up-

dated over time as business processes change. For another, the rigorous application of the least user privilege model will result in more secure data.

The one place in the least user privilege model that companies make the most missteps is with administrator access. Network and database administrators need high and wide access to data to perform their duties, but they don't need unlimited access that effectively gives them the keys to the kingdom.

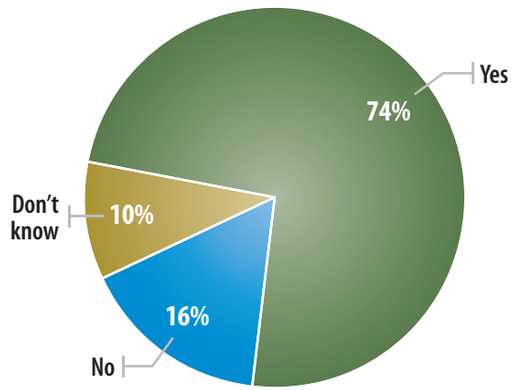
Data should be made accessible to all employees on a need-to-know basis. If they don't need the data to do their jobs, they don't need access to the data. Period. Requests for access or escalation of access must be formally documented and approved by one or possibly two people at designated levels of management, depending on the value of the information being accessed.

It's important to have checks and balances in place. They're especially helpful to have when, say, a database administrator is put in the uncomfortable position of responding to a high-ranking company exec who wants access to data that isn't deemed necessary for his or her role.

The process of assigning and maintaining role-based access isn't black and white, and at some point should involve the company's human resources department.

Check The Log

Does your company have transaction logging enabled for all databases containing sensitive information?



Data: *InformationWeek* 2010 State of Database Technology Survey of 755 business technology professionals, August 2010

But attention is needed here, as well, because IT and HR aren't always in sync, says Cobweb Applications' Cobb. For example, he says, "IT isn't told employee X is no longer responsible for Y so therefore the database role needs changing."

The Real Work Begins

Once your database is properly provisioned and hardened, the real work of maintenance begins. Many tools are available to automate the tasks associated with keeping companies' most valuable and sensitive information secure.

Monitoring and logging tools, for example, show who accessed what and when over time. Most database systems include native tools for these tasks, but third-party products can provide additional capabilities.

Database provisioning and access control will only get more challenging as time goes on and computing models evolve. The increasing use of big data, NoSQL databases, and cloud-based data storage will force IT organizations to integrate their provisioning efforts.

But the biggest challenge companies face will be keeping pace with the amount of data being generated, determining the data's value, and deciding which users need access to the data to effectively drive business goals yet meet regulatory standards.

The least user privilege model still works to help secure data. And while it's not the approach that uses the fewest IT resources possible, it does gives you effective control over your users' data access and keeps your data safe.

Write to us at iwletters@techweb.com.

dark READING *Online, Newsletters, Events, Research*

Tim Wilson Dark Reading Site Editor
wilson@darkreading.com 703-262-0680

Kelly Jackson-Higgins Dark Reading Senior Editor
higgins@darkreading.com 434-960-9899

Rob Preston VP and Editor In Chief
rpreston@techweb.com 516-562-5692

Chris Murphy Editor
cjmurphy@techweb.com 414-906-5331

Stacey Peterson Executive Editor, Quality
speterson@techweb.com 516-562-5933

Lorna Garey Executive Editor, Analytics
lgarey@techweb.com 978-694-1681

Jim Donahue Chief Copy Editor
jdonahue@techweb.com

Mary Ellen Forte Senior Art Director
mforte@techweb.com

Sek Leung Associate Art Director
sleung@techweb.com

Business Contacts

VP of Group Sales, InformationWeek Business Technology Network, Martha Schwartz
(212) 600-3015, mschwartz@techweb.com

Sales Assistant, Salvatore Silletti
(212) 600-3327, ssilletti@techweb.com

SALES CONTACTS—WEST

Western U.S. (Pacific and Mountain states) and Western Canada (British Columbia, Alberta)

Western Regional Director, JohnHenry Giddings
(415) 947-6237, jgiddings@techweb.com

Strategic Account Director, Mark Glasner
(415) 947-6245, mglasner@techweb.com

Account Manager, Kevin Bennett
(415) 947-6139, kbennett@techweb.com'\

Account Manager, Ashley Cohen
(415) 947-6349, aicohen@techweb.com

Strategic Accounts

Account Director, Sandra Kupiec
(415) 947-6922, skupiec@techweb.com

SALES CONTACTS—EAST

Midwest, South, Northeast U.S. and Eastern Canada (Saskatchewan, Ontario, Quebec, New Brunswick)

District Manager, Jenny Hanna
(516) 562-5116, jhanna@techweb.com

District Manager, Michael Greenhut
(516) 562-5044, mgreenhut@techweb.com

District Manager, Cori Gordon
(516) 562-5181, cgordon@techweb.com

Inside Sales Manager East, Ray Capitelli
(212) 600-3045, rcapitelli@techweb.com

Strategic Accounts

District Manager, Mary Hyland
(516) 562-5120, mhyland@techweb.com

Account Manager, Tara Bradeen
(212) 600-3347, tbradeen@techweb.com

SALES CONTACTS—MARKETING AS A SERVICE

Director of Client Marketing Strategy, Jonathan Vlock
(212) 600-3019, jvlock@techweb.com

SALES CONTACTS—EVENTS

Senior Director, InformationWeek Events, Robyn Duda
(212) 600-3046, rduda@techweb.com

MARKETING

VP, Marketing, Winnie Ng-Schuchman
(631) 406-6507, wng@techweb.com

Director of Marketing, Angela Lee-Moll
(516) 562-5803, aleemoll@techweb.com

Marketing Manager, Monique Kakegawa
(949) 223-3609, mkakegawa@techweb.com

UBM TECHWEB

Tony L. Uphoff CEO

John Dennehy CFO

David Michael CIO

Scott Vaughan CMO

David Berlind Chief Content Officer, TechWeb, and Editor in Chief, TechWeb.com

Ed Grossman Executive VP, InformationWeek Business Technology Network

Martha Schwartz VP, Group Sales, InformationWeek Business Technology Network

Joseph Braue Sr. VP, Light Reading Communications Network

Beth Rivera Senior VP, Human Resources

John Ecke VP of Brand and Product Development, InformationWeek Business Technology Network

Fritz Nelson VP, Editorial Director, InformationWeek Business Technology Network, and Executive Producer, TechWeb TV

UBM LLC

Pat Nohilly Sr. VP, Strategic Development and Business Admin.

Marie Myers Sr. VP, Manufacturing

READER SERVICES

DarkReading.com The destination for the latest news on IT security threats, technology, and best practices

Electronic Newsletters Subscribe to Dark Reading's daily newsletter and other newsletters at darkreading.com/newsletters/subscribe.jhtml

Events Get the latest on our live events and Net events at informationweek.com/events

Analytics analytics.informationweek.com for original research and strategic advice

How to Contact Us
darkreading.com/aboutus_editorial.jhtml

Editorial Calendar informationweek.com/edcal

Back Issues
E-mail: customerservice@informationweek.com
Phone: 888-664-3332 (U.S.)
847-763-9588 (Outside U.S.)

Reprints Wright's Media, 1-877-652-5295
Web: wrightsmedia.com/reprints/?magid=2196
E-mail: ubmreprints@wrightsmedia.com

List Rentals Merit Direct LLC
E-mail: acarraturo@meritdirect.com
Phone: (914) 368-1083

Media Kits and Advertising Contacts
createyournextcustomer.com/contact-us

Letters to the Editor E-mail editors@darkreading.com. Include name, title, company, city, and daytime phone number.

Subscriptions
Web: informationweek.com/magazine
E-mail: customerservice@informationweek.com
Phone: 888-664-3332 (U.S.)
847-763-9588 (Outside U.S.)

UBM TechWeb