Next

UBM
Tech
informationweek.com

InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY
DECEMBER 2013

The Future Of Identity

Mobile, cloud, and BYOD have blurred the lines between work and home, forcing IT to envision a new identity and access management strategy >>

By Grant Moerschel and Rick Dreger

PLUS Utilities underestimate smart grid security risks >>

Commentary

What IT Can Teach Utilities About Securing Smart Grids

ROBERT HINDEN

There is a perception within IT circles that the threats against critical infrastructure such as smart grids are a problem waiting to happen — but not right away. The reality is that last year alone, there were a number of sophisticated attacks, and they should offer a wake-up call for the power industry.

According to the Department of Homeland Security's Industrial Control Systems Computer Emergency Response Team (ICS-CERT), 41% of incidents reported and investigated by the agency last year were related to the energy industry.

Smart grids refer to the new IP networks that utilities are installing in the power grid, including substations, distribution and transmission networks, and smart meters. Utilities see a lot of advantages to smart grids, such as real-time measurement of power consumption, a better understanding of use patterns, and the ability to add and disconnect customers remotely. These improvements will generate electrical power more efficiently and in a way that better matches demand.

If the vulnerabilities and security concerns aren't addressed, however, the consequences will be terrible. An attack against a corporation would be inconvenient for the company, and online identity theft can be troublesome to an individual, but a smart grid attack would disrupt far more victims and have far-ranging effects. If a city lost power, hospitals would have to scramble to keep life-support systems on, failed traffic lights would bring traffic jams and accidents, and residents would be trapped in the dark.

A Worldwide Problem

Smart grids represent the biggest upgrade to the electrical power infrastructure in many years. In the US alone, $3.4 billion of federal stimulus funds have been slated for electric grid projects. The shift to these new networks is a worldwide trend, making cyber-attacks a global problem.

The attackers are already knocking. Last year a denial-of-service attack knocked the internal communications system of a German power utility specializing in renewable energy offline. The supply of electricity to customers was unaffected, but it reportedly took a few days to repair and bring back the email server and other communications platforms.

The traditional thinking is that smart grids are isolated networks separated from the Internet (protected with a firewall or two) and require a VPN for remote access. But this kind of perimeter security, with a hard exterior and soft interior, is not close to sufficient anymore.

The Internet is a big source of threats, but the ever-dependable USB stick is turning out to be a very common attack vector. Remember that Stuxnet, the cyber-weapon that disabled the centrifuges at Iran's Natanz nuclear facility, was initially spread via infected USB sticks.

In fact, toward the end of 2012, ICS-CERT reported that the industrial control systems at a power generation facility (which it did not name) had been infected with "both common and sophisticated malware" by a tainted USB drive. ICS-CERT investigated another malware infection at a power company in October 2012, this time in the turbine control system. This infection was also caused by a USB drive. It affected about 10 computers on the control

Sound Off

Want to raise your profile? InformationWeek is looking for technology and business strategy experts to write independent and thought-provoking opinion columns for our site. Contact managing editor Shane O'Neill to learn more.

system network and delayed the plant's reopening by three weeks.

That being said, completely isolating a smart grid network from the Internet isn't sufficient to truly protect it.

Not surprisingly, default passwords are another problem for smart grid equipment. Unless the local administrator disables the default account or changes the hard-coded default passwords, attackers will have a back door into the system. The problem is widespread across vendors. Power equipment vendors haven't learned the lessons learned elsewhere.

It's not unheard of for Windows 95 machines to run critical systems in the energy industry. IT needs to make a business case to replace these vulnerable systems.

RuggedCom's Rugged Operating System, used in many industrial control systems, has a hard-coded RSA SSL private key. The Magnum MNS-6K Management Software from GarrettCom has an undocumented hard-coded password. Siemens, the undisputed leader in this space, shipped its Synco OZW devices with a default password protecting administrative functions.

No one really knows the extent of the current problem; there haven't been a lot of cybersecurity failures reported to ICS-CERT. Energy companies and electrical equipment vendors aren't security experts. They don't know how to deal with the kind of sophisticated threats and attacks enterprise IT teams routinely face.

There are many lessons the power industry can learn from enterprise IT, including the value of implementing layers of security (such as antivirus, anti-malware, and anti-bot software) on each device and control system. Though prevailing opinion says critical power systems should never be on the Internet, putting these systems online is actually a good security step. The software can be automatically updated whenever new signatures or versions are available. Running old, outdated security software is not adequate.

Most enterprises standardize across a handful of operating systems. In the energy industry, it's not unheard of for Windows 95 machines to run critical systems. IT administrators need to make a business case to replace these older, more vulnerable, and harder-to-remediate networks and systems. Staff members need to be trained to improve their security capabilities.

There already are a number of smart grid standards, such as NERC-CIP, a federal regulation to protect critical infrastructure; IEC 61850, which covers how to secure network infrastructure; and IEEE 1613, which outlines environmental requirements for IT equipment in substations. These standards identify areas where utilities need to improve.

Securing the smart grid is essential, but it won't be easy. The good news is that the tools and resources are available for utilities to get the job done. Just ask a colleague in IT.

Robert Hinden is a Check Point Fellow and chair of the Internet Society Board of Trustees and the IPv6 (6MAN) working group at the Internet Engineering Task Force. He was co-recipient of the 2008 IEEE Internet Award for pioneering work around the first Internet routers. Discuss this article here, or write us at iwletters@ubm.com.

Previous Next

ISTOCK

The Future Of Identity

Mobile, cloud, and BYOD blur the lines between work and home, forcing IT to envision a new identity and access management strategy.

By Grant Moerschel and Rick Dreger @GrantMoerschel

The traditional worker bee comes in to the office, logs in to a dedicated computer via Microsoft Active Directory credentials, and gets access to local applications and data shares needed to conduct daily activities. Simple, familiar, controlled — and totally out of date for companies dealing with mobile devices, cloud computing, BYOD, and the blurring line between work and home, business and personal.

As mobile and cloud computing use booms, we're outgrowing our trusty old technology for identity and access management. But our future vision — to

Previous Next

know a person's identity across all the multiple devices, cloud services, and roles they have — isn't possible with today's still emerging technology. This causes tons of confusion as vendors vie to be the next great thing and IT tries to determine where to place bets. As these emerging cloud and mobile technologies settle out over the next few years, we in IT must maintain control by buying into transitional technologies, and also staking out and enforcing sometimes unpopular policies. Employees don't like passcodes on phones, or giving up their personal Dropbox storage for an enterprise option, or feeling like their company might erase personal information from a device, but adopting new technology comes at a cost. Balancing the benefits with the costs is the art of information technology.

If you're not assessing the impact that increased use of mobile devices, bring-your-own-device initiatives, cloud storage, and cloud apps are having on your identity and access management strategy, then you're falling behind. Here are some important places to start.

Two-Factor Technology With Cloud

As we move away from the model of employees only accessing on-premises software systems using company devices and networks, we also increase our exposure to certain threats. Now, instead of needing to get onto the corporate network with an approved device to access SharePoint files, we could potentially connect to Box from any device and simply provide a user name and password. The upside of the cloud option is easier access to important data, but the downside is that only a user name/password combination now stands between an attacker and company information. Not that we would *ever* accuse you or your colleagues of creating weak passwords, but we need something better.

Two-factor technologies aim to supplement poor or lost passwords by introducing a second component to the identity process. RSA and Entrust are the well-known old guard with millions of deployments, and the two-factor options range from tokens and smart cards to phone callbacks and SMS messages. Most of these technologies convey one-time passwords that are good for a period of time once you've made an authentication request to a system such as a web server, application, or VPN endpoint. OTP has been around for a long time and is better than just a password, but it's susceptible to man-in-the-middle attacks and DNS poisoning, such as when an attacker captures the OTP when someone unknowingly input it into a fake form. And it often relies on having an extra thing, such as a token or smart card.

One of the more exciting two-factor technologies we've seen that alleviates OTP weaknesses is Cyphercor's LoginTC. Say a salesperson out on the road is accessing Salesforce.com at a coffee shop. If using LoginTC, she enters her primary credentials on the site, and a message pops up on her phone asking "yes or no" if the access is legitimate. She answers yes, enters a passcode on her phone that unlocks a local token, and a message goes back to grant access.

LoginTC has two big advantages over OTP. First, Salesforce doesn't need personally identifiable information such as a phone number because tokenized challenges travel over the certificate-based Android, Apple, and BlackBerry push notification networks. Eliminating stored personal information simplifies regulatory compliance. Second, there are no vulnerable OTP codes being transmitted through insecure channels such as SMS or via automated phone calls or via cycling hardware tokens that are then entered into some remote web interface form that may or may not be legitimate. And there's a third factor: It uses the smartphone that salespeo-

Previous Next

ple already carry. Simplicity like this is key to getting employee adoption.

Better In-House Identity Tracking

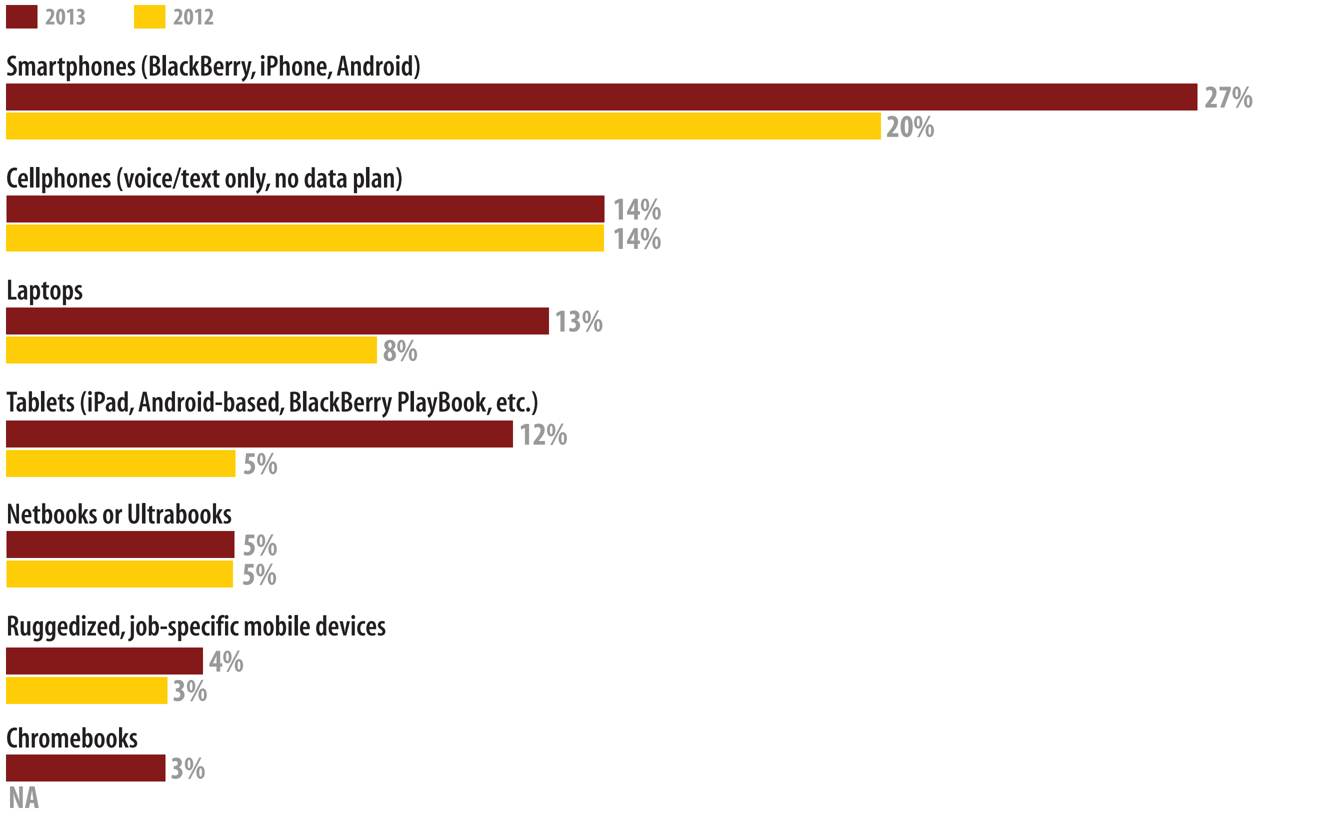
Before tackling the more difficult cloud and mobile use cases, make sure you have control of access requests coming from your corporate offices. Tackling the problems you know best with a consistent plan will give you credibility to address the tougher ones.

We see all the time basic identity and access management plans that put all their eggs in one basket — Active Directory credentials. Take a simple access scenario: An employee, Siegfried, logs in to his laptop and connects to the network with a wired connection, asserting his corporate identity with an Active Directory user name and password. All we know is he gets access to certain apps and data based on his role. We have limited visibility into Siegfried's activities on the network because firewalls traditionally limit traffic based on IP address or network range, and our in-office employees receive addresses based upon dynamic DHCP addresses taken from large pools. Further, we have very limited understanding of what device Siegfried is using since the wired networks are usually fairly "dumb" and often assume that physical access to a port is enough to permit network access.

Here's an alternative, modern office environment that's more identity-centric. When Siegfried tries to connect to the office network, whether he uses his wireless card or a wired connection, the network requires an 802.1X authentication process to validate his device. Siegfried's using a company laptop that has the device-based certificate. Siegfried still needs his tried-and-true user name and password that authenticate via Active Directory. But he gets a DHCP address that's

Personal Gadgets At Work

Which of these personally owned mobile devices are used for work by 51% or more of employees?



Data: InformationWeek Mobile Security Survey of 424 business technology professionals in April 2013 and 322 in March 2012 mapped to his credential (and thus his work identity) by both the network and the company's next-generation firewall. Now the company can log all Siegfried's network-based actions, whether internal or out to the Internet, against his identity and the device he is using. In the past, if Siegfried tried to access the accounting server but wasn't part of that team, we would rely on his login not authorizing access; with this approach, Siegfried gets denied at the network level from even attempting to talk with the accounting server.

We need to combine IAM technology with smart networks and firewalls to manage data flows in the office based on identity.

And we can extend this to external access such as Internet apps. Companies are overly generous with Internet access — free and open employee access is commonplace. This creates a nice ripe attack surface, and we think companies should consider using identity and access management to provide granular, role-based access. For example, we could permit our HR department to use Facebook all day to vet potential employees. We could choose to get more detailed and permit certain types of Facebook activities while denying others (e.g., Facebook chat). For other employees, we might permit Facebook use only at lunch, say 11 a.m. to 1 p.m., using Active Directory groups.

You get the idea: We need to combine IAM technology with smart networks and firewalls to manage data flows in the office based on your identity.

Identity And Cloud Infrastructure

Most companies will never move completely to the cloud and instead will have hybrid environments that use cloud software, public cloud infrastructure, and the highly virtualized private cloud datacenters. In those cloud environments, the crown jewels we call data run on collapsed virtual infrastructure using a reduced number of servers and one hypervisor as the underpinning. With so much reliance on software, we need to ensure that our administrators are who they say they are and that they have permission to make changes.

In contrast to a mistake made on one physical server that takes down only that server, a mistake at the hypervisor layer can cause all of your servers to go offline.

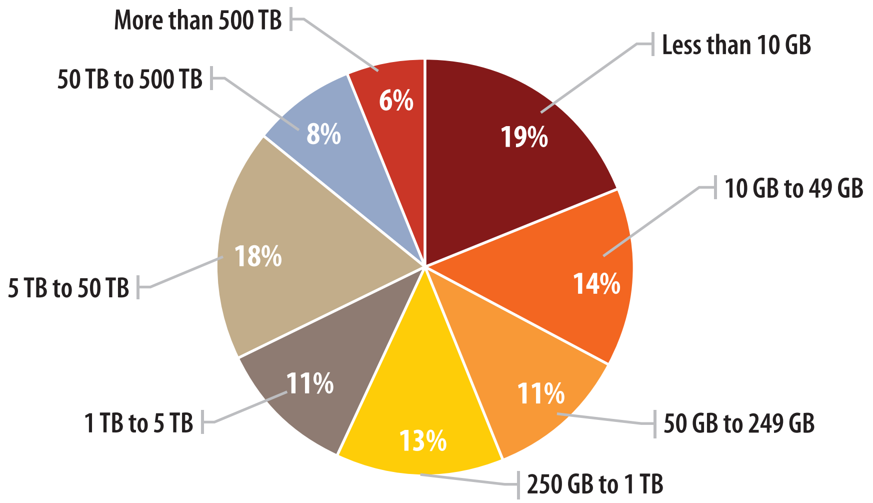
Identity and access management is vitally important for these linchpin components, but as security assessors we often see minimally protected management interfaces for critical equipment. For example, we see shared administrative accounts with god-level access, which makes it impossible to attribute changes to any one person.

"Cloud technology gives us fantastic scaling and cost savings opportunities, but it also consolidates our risk because the systems are in one place," warns Eric Chiu, president of cloud security company HyTrust. A rogue administrator could steal entire server copies, or even destroy the environment. Technology such as HyTrust's enforces role-based cloud management activities and the "two-person rule" that requires changes to be authorized by a second person. HyTrust also encrypts guest OS files (such as the VMware VMDK) so that servers can be run in a public cloud.

Ultimately, IT organizations need to look at how cloud risks affect their security strategy. You may have the most hardened servers in the world, but if they are essentially unprotected at the hypervisor's management plane because of lax identity and access controls, a rogue or fat-fingered administrator, or an attacker posing as an administrator, can cause serious damage or theft.

Storage To The Cloud

How much data does your organization store in the cloud (consider just dedicated cloud storage)?



Data: InformationWeek Cloud Storage Survey of of 225 business technology professionals at organizations using or planning to use cloud storage services, May 2013

Multiple Mobile Personalities

CIOs and their teams are in knots over how to tackle mobility. Allow us to start with some simple advice: Set your mobile device policies and let BYOD happen, but stand firm in protecting your data.

Technology already is pushing employee identity away from today's bifurcated model of a "personal" identity and a "work" identity to one blurred entity. For instance, iOS integrates calendars and mail into an all-in-one view. "We've got one life, not two," says AirWatch chairman Alan Dabbiere. AirWatch (which makes mobile device management software) sees mobile devices becoming our credit card, wallet, and car key in addition to already being our camera, movie player, and work assistant. To deal with this trend, BYOD will need "smart bifurcation."

For policies, let's start with applying a basic IAM concept to mobility — identify the person behind the device with certainty before providing resources or access. Today, the only feasible way to do that is by requiring some type of screen lock or passcode.

We hear you: Employees hate passcodes. But a passcode not only provides peace of mind should the device be lost or stolen, it's also necessary for onboard device encryption. All other mobile IAM options are a work in progress. We might one day use a thumbprint plus a voice command to unlock our devices. Perhaps the combination of face recognition via the device's camera plus our smartwatch being in close proximity will work. More flexible authentication is coming down the road, but for now you have no choice but to stand firm on mandatory passcodes.

Once our system knows who's holding the mobile device, the real work begins. What type of information should be presented and which apps are locked by default? Is there a default that shows some blended work and personal environment? IT needs workspaces or containerization to answer these questions and make BYOD a success.

Workspaces create discrete areas that a person authenticates into to get access to apps and data. Email is the best example of personal and work data integrated into one view. Entering the lock-screen password gives an employee a tidy view of her personal and corporate email in one place, but accessing certain company data takes additional authentication — perhaps to copy and paste data from messages, or to access attachments.

Taking this gated workspace idea further, we're beginning to see the creation of different workspaces for different users on the same device, such as hospital workers who share tablets across 24/7 shifts. We'll also see in the future multiple levels of authentication providing different levels of access on a device depending on the information being protected.

Mobile device management can tie remote wiping of data to workspaces, remotely deleting company data without destroying personal entries. This separation avoids malicious access, but also minimizes inadvertent access to company data while the kids are streaming a movie. We may eventually see the use of multiple phone numbers on a single device (personal and work numbers), letting organizations retain their company phone numbers when a BYOD device is terminated.

Where We Go Next

Beyond physically and logically securing mobile devices, there's an emerging IAM technology that depends on understanding user behavior to spot fraudulent access.

AirWatch and Box are each separately working on server side analytics aimed at reducing unauthorized logins. It's similar to how credit card companies use heuristic analysis and machine-learning algorithms to flag suspicious transactions. "Where we need to go to is server analytics and health checks that identify if you are coming from the same place [as usual] on the same device," Box CTO Justin Somaini says. "In this case maybe — and just maybe — no password is needed. However, if you are seen coming from a rogue state, you get no access and the attempt is flagged." Somaini notes that browser cookies are a big problem for cloud providers because a stolen cookie pre-authenticates the thief. This is similar to the one-time password theft issue noted earlier. Box has added out-of-band authentication via text messages as an option for customers, but Somaini foresees heuristics and profiling to identify abnormal access as a promising next step.

One new identity approach is similar to how credit card companies use heuristic analysis and machine-learning algorithms to flag suspicious transactions.

Another area of strong interest is centralizing the authentication of disparate cloud offerings into a secure single sign-on option for mobile users. Vendors such as Okta and Ping Identity provide SSO software that rolls together your enterprise active directory and any cloud software into a single authentication approach. A company can enroll new users and grant them access to a range of cloud software using a centralized access portal.

When the employee leaves, the system can revoke all access without touching multiple cloud logins or checking multiple authentication repositories. Companies will need these kinds of options that address convenience, complexity, and security in one swoop as they get more aggressive with mobile app access and move more of their computing to the cloud.

Grant Moerschel and Rick Dreger are co-founders of the cyber-security consulting firm WaveGard. Write to us at iwletters@ubm.com.

Previous Next

InformationWeek

Print, Online, Newsletters, Events, Research

Rob Preston VP and Editor In Chief
rob.preston@ubm.com 516-562-5692

Chris Murphy Editor
chris.murphy@ubm.com 414-906-5331

Lorna Garey Content Director, Reports
lorna.garey@ubm.com 978-694-1681

Jim Donahue Managing Editor
james.donahue@ubm.com 516-562-7980

Shane O'Neill Managing Editor
shane.oneill@ubm.com 617-202-3710

Mary Ellen Forte Senior Art Director
maryellen.forte@ubm.com

Business Contacts

SALES CONTACTS—WEST

Western U.S. (Pacific and Mountain states)

VP & National Co-Chair, Business Technology Media Sales, Sandra Kupiec
(415) 947-6922, sandra.kupiec@ubm.com

District Sales Manager, Vanessa Tormey
(805) 252-4357, vanessa.tormey@ubm.com

Account Director, Ashley Cohen
(415) 947-6349, ashley.i.cohen@ubm.com

Account Director, Vesna Beso
(415) 947-6104, vesna.beso@ubm.com

Account Director, Matthew Cohen-Meyer
(415) 947-6214, matthew.meyer@ubm.com

SALES CONTACTS—EAST

Midwest, South, Northeast U.S. and Canada

VP & National Co-Chair, Business Technology Media Sales, Mary Hyland
(516) 562-5120, mary.hyland@ubm.com

Eastern Regional Sales Director, Michael Greenhut
(516) 562-5044, michael.greenhut@ubm.com

District Manager, Jenny Hanna
(516) 562-5116, jenny.hanna@ubm.com

District Manager, Cori Gordon
(516) 562-5181, cori.gordon@ubm.com

STRATEGIC ACCOUNTS

Account Director, Jennifer Gambino
(516) 562-5651, jennifer.gambino@ubm.com

Strategic Account Director, Amanda Oliveri
(212) 600-3106, amanda.oliveri@ubm.com

SALES CONTACTS—MARKETING AS A SERVICE

Director of Client Marketing Strategy, Jonathan Vlock
(212) 600-3019, jonathan.vlock@ubm.com

SALES CONTACTS—EVENTS

Senior Director, InformationWeek Events, Robyn Duda
(212) 600-3046, robyn.duda@ubm.com

MARKETING

VP, Marketing, Winnie Ng-Schuchman
(631) 406-6507, winnie.ng@ubm.com

Director of Marketing, Monique Lutrell
(415) 947-6958, monique.luttrell@ubm.com

Marketing Assistant, Hilary Jansen
(415) 947-6205, hilary.jansen@ubm.com

UBM TECH

Paul Miller CEO

Marco Pardi President, Events

Scott Mozarsky President, Media and Partner Solutions

Kelley Damore Chief Community Officer

David Michael CIO

Simon Carless Exec. VP, Game & App Development and Black Hat

Lenny Heymann Exec. VP, New Markets

Angela Scalpello Sr. VP, People & Culture

READER SERVICES

InformationWeek.com The destination for breaking IT news, and instant analysis

Electronic Newsletters Subscribe to InformationWeek Daily and other newsletters at informationweek.com/newsletters/subscribe

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

Reports reports.informationweek.com for original research and strategic advice

How to Contact Us
informationweek.com/contactus

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 Specialists Marketing Services Inc.
E-mail: PeterCan@SMS-Inc.com
Phone: (631) 787-3008 x3020

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

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

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

UBM Tech