CMP
United Business Media

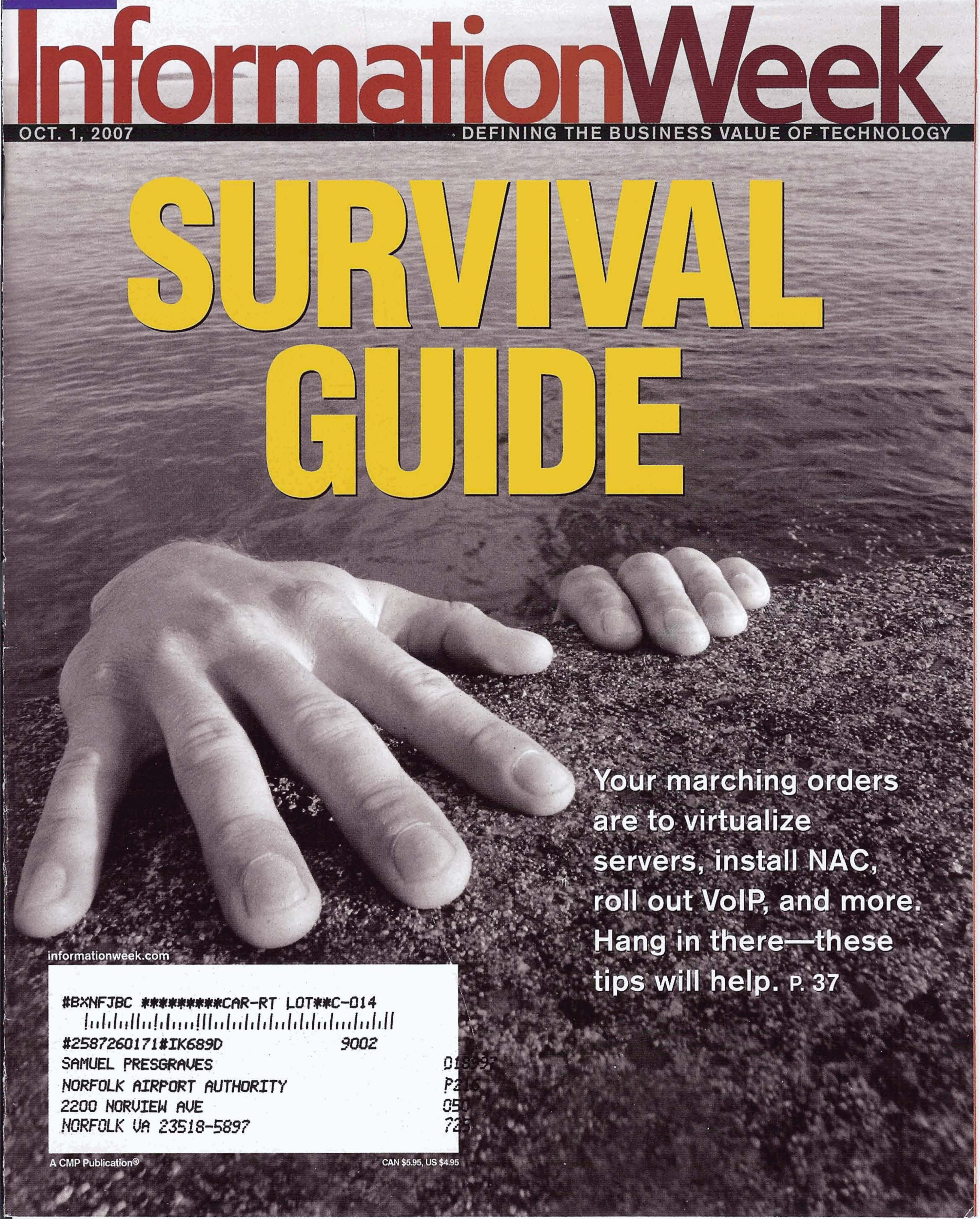
CROOK TALKS
How Robert Moore cracked VoIP P. 15

GOOGLE MOBILE
Time to prepare for the inevitable P. 19

GREEN GRID
The push for data center standards P. 49

CIOs
12 ways to lose influence P. 56

InformationWeek
OCT. 1, 2007
DEFINING THE BUSINESS VALUE OF TECHNOLOGY



SURVIVAL GUIDE

Your marching orders are to virtualize servers, install NAC, roll out VoIP, and more. Hang in there—these tips will help. P. 37

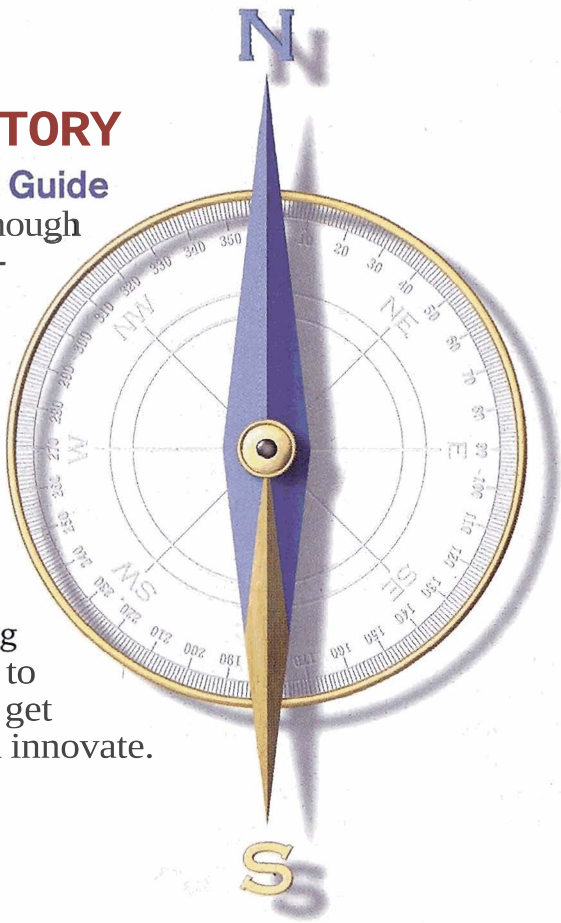
informationweek.com

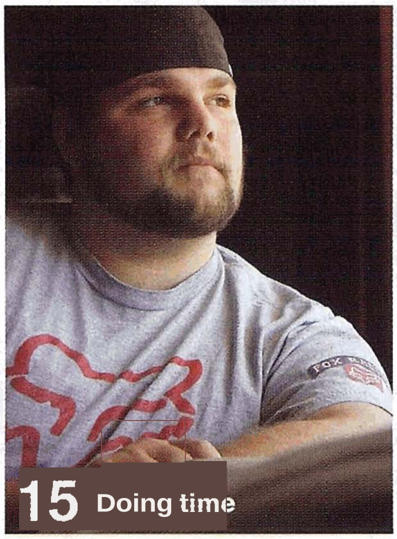
A CMP Publication®
CAN $5.95, US $4.95

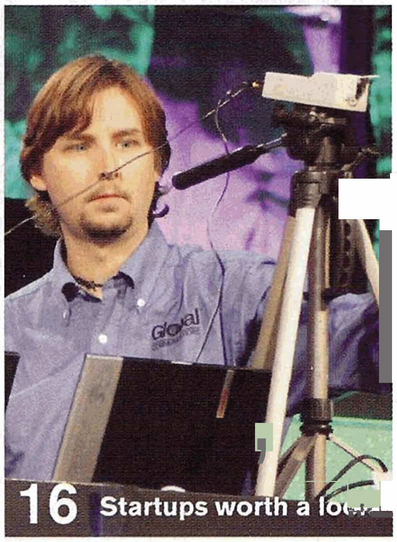
CONTENTS

InformationWeek >> DEFINING THE BUSINESS VALUE OF TECHNOLOGY ISSUE 1,156 OCT. 1,2007

COVER STORY







Cover photo age fotostock/Superstock

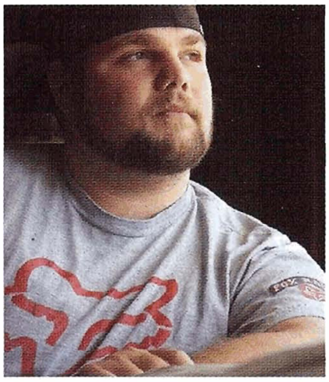
> NEWS FILTER

NEWSFILTER

A Crook Comes Clean

ROBERT MOORE, 23, of Spokane, Wash., began a two-year sentence in federal prison last week for his part in a scheme to steal and sell voice-over-IP services. While prosecutors call co-conspirator Edwin Pena the mastermind of the operation, Moore was the high-tech muscle, scanning and breaking into telecom companies and other corporations around the world.

"It's so easy a caveman can do it," Moore said, laughing, in a telephone interview with *InformationWeek* before his incarceration. "When you've got that many computers at your fingertips, you'd be surprised how many are insecure."



'If they were just monitoring their boxes and keeping logs, they could easily have seen us logged in there.'
–Robert Moore

Assistant U.S. Attorney Erez Liebermann says Pena, who fled the country a year ago and is wanted as a fugitive, allegedly stole and then sold more than 10 million minutes of VoIP services at deeply discounted rates, netting more than $1 million. As the operation's hacker, Moore said he netted only $20,000 of the haul.

The government identified more than 15 VoIP service providers that were broken into, and more.than 6 million computers scanned between June and October of 2005. AT&T reported to the court that Moore ran 6 million scans on its network alone.

THE FAULT: DEFAULT

What made the hacking job so easy, Moore said, was that 70%of all the companies he scanned were insecure, and 45%to 50%of VoIP providers were insecure. The biggest insecurity? Default passwords. "You wouldn't believe the number of routers that had 'admin' or 'Cisco0' as passwords on them," Moore said. "We could get full access to a Cisco box with enabled access so you can do whatever you want to [it]."

Moore also targeted Mera, a Web-based VoIP switch. "It turns any computer into a switch so you could do the calls through it," he said. "We found the default password for it. I'd write a scanner for Mera boxes, and we'd run the password against [them] to try to log in, and basically we could get in almost every time. Then we'd have all sorts of information, basically the whole database, right at our fingertips."

Moore described himself as a "mega geek," more upset about being denied the use of a computer than going to prison. His job in the operation largely was to write software that ran scans and brute-force attacks against Cisco XM routers and Quintum Tenor VoIP gateways. To do that, he used 2 Gbytes of information on corporate IP ranges that he bought on the black market for $800.

He would first scan the network looking mainly for the Cisco and Quintum boxes. When he found them, he'd scan to see what models they were and then scan again for vulnerabilities, such as default passwords and unpatched bugs in old Cisco IOS boxes. If he didn't find default passwords or easily exploitable bugs, he'd run brute-force and dictionary attacks to try to break the passwords.

"We would go to telecom forums and other telecom sites that list company names and where they're from," he explained. "We'd look at foreign countries first. We'd take the name and IP range and then dump it into the scanner. ... Some of the Cisco versions, like IOS, were old and easier to get into."

Prosecutor Liebermann notes that while Moore broke into telecoms to steal VoIP service, he also hacked into other businesses so he and his partner could use hijacked company connections to disguise the calls they were sending to the telecoms.

Moore said it would have been easy for IT and security managers to detect him-if they'd been looking. "If they were just monitoring their boxes and keeping logs, they could easily have seen us logged in there," he said. "If they had intrusion-detection systems set up, they could have easily seen that these weren't their calls."

IT technicians also could have set up access lists, telling their networks to allow only their own IP addresses to get in. "We came across only two or three boxes that actually had access lists in place," Moore added. "The telecoms that we couldn't get into had access lists or boxes that we couldn't get into because of strong passwords." —SHARON GAUDIN (sgaudin@cmp.com)