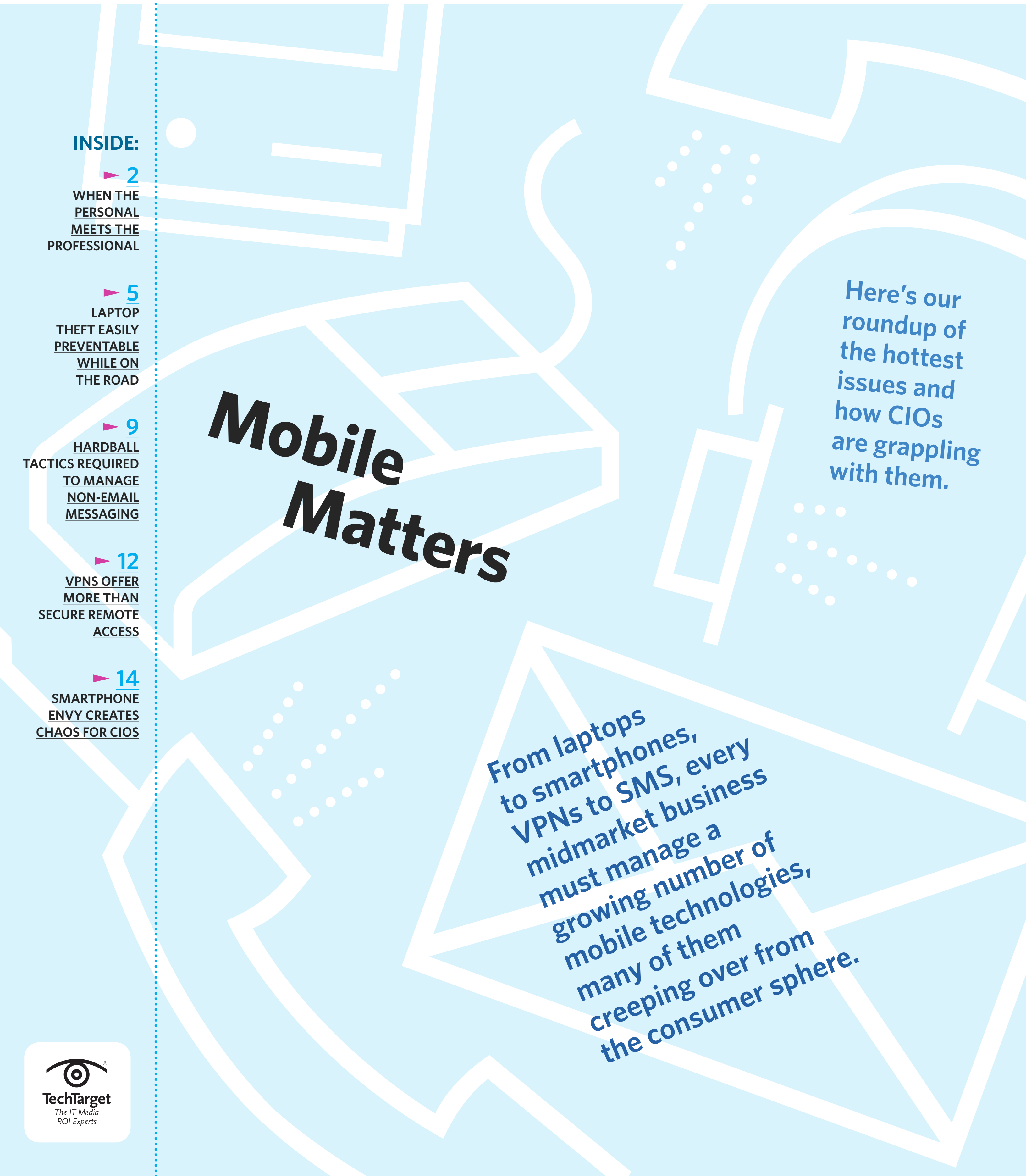
SearchCIO-Midmarket.com

Technology Management Strategies
for the Midmarket CIO



INSIDE:

Mobile Matters

Here's our roundup of the hottest issues and how CIOs are grappling with them.

From laptops to smartphones, VPNs to SMS, every midmarket business must manage a growing number of mobile technologies, many of them creeping over from the consumer sphere.

TechTarget
The IT Media ROI Experts

When the Personal Meets the Professional

As employees lobby for consumer devices at work, CIOs must find ways to accommodate them—or just say no.

BY ZACH CHURCH

IT IS THE allure of smartphones as status symbols, "objects of desire" as Gartner Inc. research vice president Monica Basso calls them, that is pushing them from the business world into the consumer world, and vice versa.

As the wireless industry hits its stride—connections are everywhere, and Gartner research shows IT leaders are less and less concerned about security each year—the consumer and business worlds are on a collision course.

Many employees, enamored of their new, tricked-out personal phones, want them synced up with their work networks. And more will be asking for that privilege.

The first reaction, of course, is to say "No." Why compromise security and take on a series of network headaches so the hipper component of the company workforce can look cool?

That's a fair question, Gartner analyst and vice president Nick Jones said. But with well-enforced policies and employee education, CIOs should be encouraged by the blurring of the line between work device/play device, Jones said.

"Don't say no as a gut reaction," Jones said, speaking at Gartner's 2008 Wireless & Mobile Summit. "I don't think we can or should always resist demand from employees who may want some corporate applications on employee-owned devices."

Take the BlackBerry. Research In Motion (RIM) President and co-CIO Mike Lazaridis said his company, which manufactures the popular smartphone, still sees business as the sweet spot. But the BlackBerry is no secret outside of work, and more and more people are buying the phone for personal use. Windows Mobile devices and other smartphones are also starting to gain traction.

"They're literally walking into the stores and asking for a BlackBerry," Lazaridis said. Recently, RIM integrated social networking service Facebook into its phones.

"They bought [a consumer device] and they want to use this device to connect to corporate email and corporate data," Basso said. "Theoretically, an enterprise should completely ban the use of iPhone. The reality is, if you do this, what happens is the iPhone users will find other ways to access their email."

In March, Apple Inc. announced

WHEN THE PERSONAL MEETS THE PROFESSIONAL

LAPTOP THEFT EASILY PREVENTABLE WHILE ON THE ROAD

HARDBALL TACTICS REQUIRED TO MANAGE NON-EMAIL MESSAGING

VPNS OFFER MORE THAN SECURE REMOTE ACCESS

SMARTPHONE ENVY CREATES CHAOS FOR CIOS

that the iPhone will now work with Microsoft ActiveSync, part of a strategy to bring enterprise customers to what was previously a consumer-only device. Apple also launched its iPhone software development kit, allowing the creation of third-party applications for the phone.

Analysts Jones and Basso recommend CIOs familiarize themselves with the most popular consumer products—both wireless and Web-based, such as Facebook and MySpace—and develop a series of policies for their use in the workplace.

Manufacturers of consumer-cum-business products are constantly pushing them toward employees, and sooner or later the IT department has to deal with them, said Steve Vandermolen, an IT director at Grand Rapids, Mich.-based restaurant supplier Gordon Food Service.

"We look at ways to embrace [them]," Vandermolen said. Gordon Food Service is comfortable with employees using personal BlackBerrys, provided they adhere to company use policies.

Vandermolen said caution and oversight are key when IT begins sanctioning user-owned smartphones and other wireless products. And companies shouldn't allow their use if there is no real business value, he said.

"Some of them are fads and they don't last long," he said.

Jones and Basso said staying open minded isn't only a must, but it can also benefit the business. Business innovation, so often directed from above, might spring up in the lower ranks by employees finding easier ways to complete tasks using consumer products, Jones said.

There is some evidence that CIOs are willing to loosen the reins. A late 2006 Gartner survey of 150 IT directors in Australia found that 72% expected personal smartphones and digital assistants to be sanctioned in the workplace by 2010.

> "Some [mobile products] are fads and they don't last long."
> —STEVE VANDERMOLEN, IT DIRECTOR, GORDON FOOD SERVICE

And about half of 97 U.S. CIOs surveyed by Gartner late last year said they were satisfied with the ability of consumer-oriented products and applications to contribute to business success (although another survey found that about 90% of CIOs want to ban Facebook).

Besides security precautions CIOs should begin developing policies for personal-device use and build and enforce a list of unauthorized devices, Basso said. Conversely, she suggested building a list of approved devices and encouraging employees to purchase them. Educating employees about secure use of personal wireless toys is also a must, she said. ■

Zach Church is a news writer for SearchCIO-Midmarket.com. He can be reached at zchurch@techtarget.com.

Dr. John Halamka

CIO and Emergency Room Physician

Ask Dr. John Halamka Why He Loves His BlackBerry

"I'm the CIO of Harvard Medical School and four hospitals, and I'm also an emergency room physician. Any device I use personally and deploy widely has to be flexible, intuitive, and offer advanced security and systems integration. My BlackBerry® and the 500 other BlackBerry smartphones I support in our organization deliver on all of that. That's why all my direct reports and key operations people have them. My BlackBerry allows me to be as responsive as I need to be. It's industrial strength–yet very easy to use."

Find out why people love BlackBerry, or tell us why you love yours, at www.blackberry.com/ask.

BlackBerry®

AN EXPERT VIEW

Laptop Theft Easily Preventable While on the Road

This security primer will help you keep your mobile devices out of the hands of thieves.

BY JOEL DUBIN

AS THE TECHNOLOGY for mobile computing becomes more efficient and less expensive, the number of workers working remotely is increasing rapidly. Unfortunately, so are the security risks.

Midmarket companies without the resources for complicated and expensive network access control systems or endpoint security products are particularly vulnerable to breaches from lost or stolen laptops. And as we hear every day now in the news, stolen or lost laptops with confidential customer information or sensitive company data can cause incalculable damage to a company of any size.

Fortunately, there are solutions that don't require expensive hardware or software and can protect both laptops and the networks to which they connect. By using an established set of policies and procedures combined with some reasonably priced and easy-to-deploy products, IT organizations no longer have an excuse for sloppy mobile computing security practices.

For midsized companies, there's a two-pronged approach to securing laptops that I think works best.

First is the low-tech approach. This involves teaching the basics of laptop safety—never leave your laptop unattended, use privacy filters to prevent shoulder surfers and other wandering eyes from stealing user IDs and passwords, and be aware of your surroundings. A little bit of education goes a long way. Put this information in a PowerPoint presentation or a company policy and make sure mobile workers sit through a review of this policy once a year as a condition of employment.

While laptop theft at airports is rampant, there is just as much risk in hotel rooms and rental cars. In hotels, it's probably best to take a laptop with you rather than leave it in the room unattended. As for rental cars, laptops shouldn't be left on car seats where they can be seen during appointments or visits to client sites. Make it a policy to lock a laptop in the trunk. Better yet, lock it in the trunk via cable to the spare tire.

When traveling, especially through airports, have employees carry laptops in briefcases, not in easily identifiable laptop carrying cases. Briefcases, carrying cases and the laptops themselves shouldn't have company markings, corporate logos or other features making them stand out. Your marketing department might not be happy with the lack of public exposure of the company's brand, but it'll be another step to keeping laptops out of the wrong hands. Laptops, like employees, should blend in with the crowd as much as possible when on the road.

ON THE TOOLS FRONT

My second approach is using security tools, such as antivirus protection, firewalls and virtual private network (VPN) software. The first rule of working remotely is to use only a company-issued laptop both out of the office and when connecting to the network.

Every company laptop should have a standard build that your IT department reviews and approves to ensure it meets information security standards. That means it should have updated antivirus protection, personal firewalls and VPN software for communicating back to the network.

As the CIO, you should have a complete inventory of all laptops in use at the company. At the very least, have a list of makes, models, serial numbers, dates of purchase, the employee to whom each laptop was given and the date of issuance. If possible, barcode every laptop before it goes out the door, preferably with something tamperproof or even engraved on the case. You can't secure what you don't know you have, and a full accounting of where all your laptops are and who has them is vital to implementing any security controls.

Employees using laptops outside the office, whether at home or on the road, should be allowed to access the company network only by mobile VPN. If an IPSec VPN is too cumbersome for a smaller company, consider a Secure Sockets Layer VPN, which is just a Web-based VPN without some of the extra client software and hardware of its heavier-weight IPSec counterparts (see also "VPNs Offer," page 12).

VPN access also protects the network from laptop users connecting from wireless access points, which are now common in airports and hotels. Public wireless hotspots are notoriously insecure—and frequently unencrypted—but a VPN creates a secure encrypted tunnel that lowers the risk tremendously.

ENCRYPTION IS BEST DEFENSE

Now, despite all these controls, be forewarned: Laptops will get stolen. You can bet on it. So the best way to protect your company's data is full-disk encryption (FDE). With FDE, all the data on the laptop is constantly encrypted behind the scenes while the user is working. When the user shuts down, the entire hard drive is encrypted. When the user boots up again, he or she is prompted for a password that unlocks the machine. To a laptop thief without the password, the data on the disk will appear as gibberish.

A market leader in FDE is SafeBoot Technology N.V., which is now part of McAfee Inc. SafeBoot is geared to companies of all sizes and comes complete with management tools for centralized control of laptops by your IT staff. Another commercial product offering centralized management is PGP Desktop Professional.

Two popular free tools, similar to SafeBoot but lighter weight, are TrueCrypt and FreeOTFE. Both provide either full or partial disk encryption but don't offer the same centralized management options of a commercial product, like SafeBoot or PGP. But if you have a limited number of laptops to manage, free encryption tools might be a good option.

The ABCs of VPNs

- **Mobile VPN** A network configuration in which mobile devices such as notebook computers or personal digital assistants (PDAs) access a virtual private network (VPN) or an intranet while moving from one physical location to another.

- **Secure Socket Layer (SSL) VPN** A form of VPN that can be used with a standard Web browser. In contrast to the traditional IPsec VPN, an SSL VPN does not require the installation of specialized client software on end users' computers.

- **Short Message Service (SMS)** A service, commonly referred to as text messaging, for sending short messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile devices, including cellular phones, smartphones and PDAs.

- **Unified threat management (UTM) platform** Multifunction devices that combine many security applications—firewall, VPN, intrusion prevention system, Web filtering and antivirus—into a single hardware platform.

—SOURCE: WHATIS.COM

A POLICY FOR POLICIES

All of these aforementioned suggestions should be enshrined in your company's IT security policy. Though policies are only as strong as the paper they're written on, they at least are a guide to what's expected of employees if a question comes up. And written policies, at least, rather than verbal directives, can (and should) be enforced.

Finally, have an incident response plan in case a laptop is lost or stolen. Have a number employees can call 24/7 to report a missing laptop. There should be an on-call rotation schedule with someone able to take action, to notify the police if necessary, mark the laptop as missing in the inventory and, if possible, wipe or disable the laptop remotely. ■

Joel Dubin, CISSP, is an independent computer security consultant. He is a Microsoft MVP specializing in Web and application security, and is the author of *The Little Black Book of Computer Security*, available from Amazon.com. He has a regular radio show on computer security on WIIT in Chicago and runs The IT Security Guy blog at www.theitsecurityguy.com.

WHEN THE PERSONAL MEETS THE PROFESSIONAL

LAPTOP THEFT EASILY PREVENTABLE WHILE ON THE ROAD

HARDBALL TACTICS REQUIRED TO MANAGE NON-EMAIL MESSAGING

VPNS OFFER MORE THAN SECURE REMOTE ACCESS

SMARTPHONE ENVY CREATES CHAOS FOR CIOS

Hardball Tactics Required to Manage Non-Email Messaging

Instant and text messaging, or SMS, may be simplified ways of communicating. But, if left unmanaged, they could become a nightmare for IT.

BY JAMES M. CONNOLLY

EVEN IF YOU can decipher something like "b gr8 2 c u 2m" (loosely translated as "It will be great to see you tomorrow"), do you know what is really being said in all those text-based messages employees are punching into their cell phones? For that matter, do you have a handle on instant messaging in general in your organization? If you answer "no" to either question, you aren't alone.

Introduced almost a decade ago, the two messaging formats, instant messaging (IM) and Short Message Service (SMS), or text messaging, are conversational in tone and link between the cell-based text world and the IP-based instant messaging environment. Both formats also entered the corporate world without the blessing of IT and network managers, and both have the potential to circumvent information security systems.

"Instant messaging clearly presents major challenges, and people aren't even starting to address SMS," said Ted Ritter, a research analyst at Nemertes Research Group Inc. If users transmit or receive confidential company information or any content that could factor into a legal action, "they are exposing the company to potential issues," he said. And IM and SMS communications typically aren't archived, even as call records, for future retrieval in response to a lawsuit or regulatory actions.

Ritter said even people who aren't actively participating in SMS messaging may find themselves receiving text messages through clients such as Research In Motion Ltd.'s BlackBerry, as well as standard cell phones.

A GROWING CHALLENGE

Watch for SMS to present even more of a challenge in the future. It has not only gained popularity in the experienced U.S. workforce, but it may also be a staple of life for the future workers who are of college and high school age today and for all age groups in Europe and Asia. Research firm IDC estimates that there were 102 million SMS subscribers in the U.S. in 2006—one third of them business users—with that total expected to reach 184

WHEN THE PERSONAL MEETS THE PROFESSIONAL

LAPTOP THEFT EASILY PREVENTABLE WHILE ON THE ROAD

HARDBALL TACTICS REQUIRED TO MANAGE NON-EMAIL MESSAGING

VPNS OFFER MORE THAN SECURE REMOTE ACCESS

SMARTPHONE ENVY CREATES CHAOS FOR CIOS

million subscribers in 2011. However, the number of messages sent will climb even faster, according to IDC, growing from 157 billion in 2006 to 512 billion in 2011.

CIOs and their staffs have to stay ahead of that wave, Ritter said. "The whole issue is electronic information. Once it's in electronic format it's discoverable [in a legal action], and IT needs to be dealing with it on the front end, not the back end."

So what do IT professionals need to do to protect their companies from messaging misconduct?

Craig Mathias, principal of Farpoint Group, a consultancy, said that IT must acknowledge that IM and SMS are out there and will have to be managed. However, adequate management and auditing tools may be five years away. So he tells clients to "discourage your users from using instant messaging, and don't buy them an instant messaging plan or SMS plan on their cellular network. As a matter of policy, force everyone to use email."

Ritter said many companies are banning what is commonly called "public IM," the free downloads from America Online, Yahoo Inc. and others, as well as the instant messaging-like capabilities in about 100 other applications, such as Facebook. Those companies are replacing public IM with enterprise-class IM systems that feature archiving capabilities but also restrict messaging communications to company employees or approved third parties.

For employees accustomed to unlimited messaging access, a hamstrung version of IM or an SMS-less cell phone may seem unjust. Ritter and Mathias agree that it is crucial that messaging policies be carefully thought out and communicated.

MAKE PEOPLE ACCOUNTABLE

Ritter said IT must first identify where messaging is being used—and why—to identify areas for corporate exposure. Then, if there is a danger of confidential information being mishandled, IT should work with the corporate legal department or compliance office to define new policies. "It comes down to the exposure to the corporation and trying to get people to be accountable for their role in the company culture. It has to start with education," Ritter said.

Mathias added, "Whenever you communicate a policy, there are several ways you can do it. One is to say, 'If you do something wrong we'll fire you.' The other is to say, 'We don't want to use this technology because it doesn't create an audit trail, which we need for industry reasons and internal control reasons. And, it's not secure, and we have to make sure that all of our information is property managed.' If you explain it nicely up front, most people will deal with that."

James M. Connolly is a contributing writer based in Norwood, Mass. Write to him at editor@searchcio-midmarket.com.

Your business is on the move.

Your applications should be, too.

BlackBerry is your mobile solution.

The BlackBerry® solution advantage is that it keeps your mobile employees in touch with the information, customers and colleagues that drive your business. Whether email, calendar and PIM, or mobile extensions of your CRM, field service, business intelligence or collaboration tools, the BlackBerry® Enterprise Solution offers everything you need to mobilize your organization. Designed with security and flexibility in mind, the BlackBerry Enterprise Solution provides a proven, secure, open architecture for globally extending wireless communications and corporate data to mobile users.

For more information on how the BlackBerry solution can help mobilize your business visit www.blackberry.com/go/mobilizeyourbusiness

BlackBerry®

WHEN THE PERSONAL MEETS THE PROFESSIONAL

LAPTOP THEFT EASILY PREVENTABLE WHILE ON THE ROAD

HARDBALL TACTICS REQUIRED TO MANAGE NON-EMAIL MESSAGING

VPNS OFFER MORE THAN SECURE REMOTE ACCESS

SMARTPHONE ENVY CREATES CHAOS FOR CIOS

VPNs Offer More Than Secure Remote Access

Now de rigueur for offsite workers, virtual private networks also offer protection in-house.

BY MIKE ROTHMAN

IF YOU CONNECT to your company's internal network from a remote location, you should use a virtual private network (VPN)—period.

VPNs encrypt your sensitive traffic and require strong authentication, providing safe remote access. VPNs are also easy to acquire and use. The technology is mature, it's integrated into your firewall or unified threat management (UTM) platform, and it works relatively hassle-free.

SSL VPNS PREFERRED

Over the past few years, there has been a migration from IP Security VPNs to Secure Sockets Layer (SSL) VPNs because SSL VPNs don't require a specific client on the end device. That makes deployment a bit easier, but the user experience (once configured) is roughly the same. More organizations are using VPN technology to connect their remote sites and using inexpensive Internet bandwidth. This allows midmarket companies to adopt the technology more readily.

But remote access and site-to-site connections are not all that VPN technology has to offer. VPNs can be used for other reasons in an organization:

- **Visitor and/or guest access.** When consultants, auditors or other outsiders show up and want to connect to your network, all of the network jacks in conference rooms should be put on a closed network and directed into a VPN concentrator. This allows you to require strong authentication to get onto the network, ensuring that only authorized users can access internal network resources.

Another benefit of encrypting the connection for guests is if your physical network is compromised, a hacker cannot detect any authentication information by sniffing the network.

- **Wireless networks within your building.** I've seen a trend toward turning off the wired ports in most conference rooms and requiring use of the wireless. This ensures that misconfigured network ports don't allow a free pass onto the internal network.

The deployment model is similar to guest access in that all traffic on the wireless network is run through the VPN concentrator. Many UTM vendors are starting to provide integrated Wi-Fi access points in their platform. This makes a lot of sense because by definition all traffic would be routed through a VPN, providing encryption and authentication.

POINTS OF CAUTION

So what's the catch with these approaches? Aside from the cost of installing a few more boxes depending on traffic volumes, there isn't one. And with the price of access points and VPN concentrators continuing to come down, cost is becoming less of an issue.

There is one area of caution that bears mention, however. I don't recommend that organizations encrypt traffic on their internal networks. Not even between sensitive applications. Why? Encrypted data cannot be scanned and monitored for private data leakage or virus/worm proliferation.

Given the increasing scrutiny of regulations, even for midmarket companies, an organization must be able to inspect data as it travels through the network—before it is ultimately sent out into the harsh world—to ensure compliance.

But for providing access to your internal networks from outside your facility, inside conference rooms or over public wireless networks, you can't beat the security and convenience of VPN technology. ■

Mike Rothman is president and principal analyst of Security Incite, an industry analyst firm in Atlanta, and the author of *The Pragmatic CSO: 12 Steps to Being a Security Master.* Get more information about *The Pragmatic CSO* at www.pragmaticcso.com, read his blog at http://blog.securityincite.com, or reach him via email at mike.rothman@securityincite.com.

PODCAST: **TEXTING TABOO**

Texting isn't just something your kids do. In fact, **Short Message Service** (SMS), more commonly known as text messaging, is increasing in popularity within midmarket organizations and becoming the collaboration tool of choice among co-workers. But while it's less expensive than mobile email, it does have limitations, such as length of message. Regardless, SMS is something midmarket CIOs should be leveraging, not banning. This podcast with expert **Craig Mathias** examines the pros and cons of instant messaging, including costs, policies and available services.

To listen to the podcast, click here.

Smartphone Envy Creates Chaos for CIOs

Everybody (including your CEO) wants an iPhone. But caving into technology envy could put your IT department in peril. Why (and where) some CIOs draw the line.

BY MICHAEL YBARRA

BELIEVE IT OR not, when a CEO asks a CIO for an iPhone, the answer more often than not is, "No."

Steven W. Agnoli, CIO at Pittsburgh-based law firm K&L Gates, said many senior lawyers have asked for Apple Inc.'s sexy iPhone, but the IT department always replies with a polite "no."

The decision is principally because of security concerns.

"Our lawyers and staff are receptive to the fact that we have certain standards in place and it's in the firm's best interest overall to follow them," Agnoli said. "When we explain the reasons behind our policies and why a certain piece of technology doesn't match, there really isn't a problem. Our approach to overall standardization assists in these specific areas as well. We only allow a few types of units. We don't allow anything under the sun. We can't support the world. A standard platform worldwide really helps."

But midmarket CIOs should get used to the question, which they are likely to hear more and more. Apple released the iPhone last June, and by the end of the fourth quarter it had already grabbed a 28% share of the U.S. market for smartphones, according to U.K. research firm Canalys. Research in Motion Ltd.'s BlackBerry continues to dominate the market with a 41% share, while Palm has slipped to 9%.

The corporate market is a somewhat different story, with BlackBerry gobbling a 73% share, according to research firm ChangeWave, while iPhones account for only 5%. Yet corporate users report greater satisfaction with iPhones (59%) than with BlackBerrys (47%).

THE HEADACHES BEGIN

The growing popularity of mobile devices designed for consumers, not corporate users, means more headaches for CIOs.

Leslie Fiering, an analyst at Stamford, Conn.-based Gartner Inc., noted that many consumer devices are developed without remote kill features or encryption, making them too risky for enterprise users.

"The iPhone is very attractive," Fiering said. "Executives want them and the CIO's job depends on keeping them happy. But there is a cost to the company for 'executive jewelry.' This is a problem CIOs are trying to figure out. Saying no often doesn't work."

Patrick Wise, vice president of advanced technology at trucking company Landstar Systems Inc. in Jacksonville, Fla., knows the feeling.

"One of my biggest challenges is technology envy," Wise said. "Everyone wants the latest, greatest technology, but that's just not practicable every time a new toy comes out. You just can't drop $500 on a new BlackBerry every time one comes out. Keeping the users happy is hard. I can't tell you how many people have come up to me wanting an iPhone. It's not what we support. We give them the tools to support their job and environment."

Apple, meanwhile, is trying to make the device more appealing for corporate users. In March, for example, Apple announced several iPhone upgrades, such as a remote lock and erase capability and the ability to work directly with Micrsoft's Exchange software, as BlackBerrys already do.

Many CIOs, however, continue to have reservations.

MORE DUE DILIGENCE NEEDED

Agnoli, for one, said the IT department would still require quite a bit of due diligence before considering adoption.

"Apple's recent announcement regarding the iPhone may make it a more suitable platform for corporate users and it's certainly a step in the right direction for corporate use," Agnoli said. "But we'd want to review the overall capability of the platform from a network security perspective, understand the infrastructure necessary to support such devices firmwide, and decide if we would want to bring under support an additional mobile device platform and all that entails. We would do all three steps before we'd bring any new mobile device platform into the firm."

Moreover, Wise said, the price is still prohibitive.

"The iPhone isn't a corporate product," Wise said. "We can't get corporate discounts."

At Landstar, IT supports several hundred corporate users. And there are strict standards and schedules for what the company will spend for phones and personal digital assistants and when they can be replaced or upgraded.

Although there is some wiggle room.

"We'll allow people to spend their own money on cell phones; it's a very emotional thing," Wise said.

But not on the iPhone, which is available on only one wireless carrier, which offers no corporate calling plans.

What if the CEO personally asked Wise for one?

"He'd probably get one," Wise admitted, "but no one else would." ■

Michael Ybarra is a monthly columnist for SearchCIO-Midmarket.com. Contact him at editor@searchcio-midmarket.com.

RESOURCES FROM OUR SPONSOR

BlackBerry™

About Blackberry

Industry-leading BlackBerry® solutions connect people to business information, colleagues, friends and family. They offer mobile users award-winning access to email, phone, instant messaging, web, text messaging (SMS and MMS), organizer and more. Whatever your needs, there is a BlackBerry solution that's right for you.

- What's your Mobility Quotient? Click here to learn more
- Get The Facts on BlackBerry Solutions—the most widely security accredited wireless solution in the world
- For more mobile solutions click here: www.blackberry.com