Keeping Remote Users
Safe Makes Sense

Businesses must comply with government and industry regulations to avoid fines and penalties. However, tight security is a reward unto itself.

Your mobile workforce, who access your network from multiple devices (PDAs, smartphones, Blackberry devices or notebooks) from the inside, present a different variety of security threat when working outside of corporate confines. It is essential to protect your network from these potential new mobile security breaches.

The obvious reason is that without this security, company data or systems may be compromised, resulting in anything from stolen information to lost productivity to system outages. If news of a security breach gets out, it is likely to result in lost sales, lost customers and for publicly-owned companies, a decline in stock price.

A security breach due to, or revealing, a lack of compliant security could mean even larger fines and penalties — far more than the cost of security technologies that would have prevented these breaches. Even if no breach has occurred, noncompliance turned up by an audit could result in fines and penalties.

It's increasingly important that companies of all sizes and types make efforts to comply with applicable government and industry regulations, as well as implement security for their own sake.

Some of the more commonly known privacy and security regulations requiring compliance include the Health Insurance Portability and Accountability Act of 1996 (HIPAA); the Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes-Oxley); the Gramm-Leach-Bliley Act of 1999; and the Payment Card Industry (PCI) Data Security Standards. Another is California SB 1386, which mandates that companies notify any California residents if personal data is potentially exposed, for example, by theft or loss of a backup tape or notebook computer. SB 1386 applies even if your company isn't based in California. Thirty more states now have similar laws to SB 1386.

Complying With Security Regulations

Unfortunately, there is no single point of reference that medium- and even some large-sized business can go to, to determine what's needed for compliance, according to Joe Levy, CTO, at SonicWALL. Because many compliance requirements are situational, Levy notes, "A company with one vendor's equipment may be in compliance, while another company with the same setup — but different usage — may be out of compliance."

"The biggest of companies can put together compliance task forces," Levy adds. "Others normally can't, so for now they have to rely on vendors to provide them with a set of capabilities and features that can assist them in achieving compliance."

However, says security consultant Ben Rothke, author of "Computer Security: 20 Things Every Employee Should Know" (McGraw-Hill, 2006), "Security and privacy regulations like Sarbanes-Oxley, Gramm-Leach-Bliley, and Securities and Exchange Commission Rule 17a all deal with the same fundamental issues of computer security and privacy. There's around 80 percent commonality in these regulations in terms of what they're mandating."

Rothke suggests rather than trying to comply with each appropriate regulation, "The most pragmatic way to handle regulations is to create an effective information security foundation and infrastructure. This will allow your organization to also deal with new regulations as they come into law."

Merely complying with a regulation isn't necessarily sufficient to insulate your company from legal risks, cautions Daniel J. Langin, an attorney specializing in compliance issues. "Complying insulates you from that particular standard or regulation, but there's also the common law of negligence, which provides that you have to do what a reasonably prudent person would do under the circumstances. Otherwise, you still face the specter of a negligence lawsuit, usually in the form of a class-action lawsuit."

For example, in regulated industries, Langin says, "A particular standard of compliance, such as HIPAA, is a good starting point, but you can't do just that. You also have to do what a reasonably prudent company would."

Fortunately, products that provide security are increasingly available. Not

surprisingly, the products, policies and procedures needed for secure activity are also likely to address regulatory compliance requirements.

The short list of security technologies that addresses most compliance regulations for remote access, according to Rothke, include:

- SSL (Secure Sockets Layer), IPSec (Internet Protocol Security) VPN (Virtual Private Network), or SHTTP (Secure Hypertext Transfer Protocol) for Web-based access
- Endpoint security including antivirus, antispyware and firewall
- Two-factor authentication
- Access control and encryption

SSL VPNs Help Ensure Secure Connections

VPNs using SSL technology let remote and mobile users establish secure Web sessions from just about any Web browser to read e-mail and access intranet Web portals. Employees on computers that allow them to Web-download a small ActiveX or Java SSL "thin-client" applet can set up an SSL VPN connection. It's similar to an IPSec-based VPN, which lets users access authorized resources such as files, databases and applications.

SSL VPN appliances, and combination firewall/VPN or unified threat management (UTM) appliances, are becoming increasingly affordable and are available from network vendors such as Cisco, Juniper Networks, NETGEAR, SonicWALL and WatchGuard.

"You want your mobile users to use virtual private networks, so that everything they do, like e-mail or network shares, is encrypted," says Corey Nachreiner, network security analyst, at WatchGuard. "You get confidentiality. If someone tries to eavesdrop, they can't read what you're sending or receiving. And you get message integrity, meaning you can be sure that what arrives is what was sent. Our Firebox SSL Core VPN Gateway helps meet compliance »

regulations, like those specified by HIPAA, by using sufficient types of encryption, 128-bit or greater."

WatchGuard's Firebox SSL Core VPN Gateway can provide up to 205 concurrent SSL tunnels, working with the Web-download on-demand client. It also allows up to three kiosk-mode sessions suitable for e-mail or other Web-based activities through any secure browser.

SonicWALL offers both SSL VPN and UTM appliances. The company's TZ appliances provide small-office-suitable firewall, intrusion prevention, antivirus/spam and SSL VPN. Higher-end TZ models also integrate wireless switch controllers to manage wireless access points in the office.

For companies looking to add SSL capabilities, SonicWALL offers its SSL-VPN 200, for up to 10 concurrent users; the SSL-VPN 2000, for mid-sized organizations up to 500 people and a recommended maximum of 50 concurrent users; and the SSL-VPN 4000, for up to 200 concurrent tunnels. SonicWALL's PRO Series firewalls are also available.

Securing Gateway Access With NAC and Endpoint Client Security

Two increasingly popular ways that companies are tightening security are Network Access Control (NAC) and endpoint client security.

NAC interposes a layer of authentication and lets companies define who, or what groups of users, are allowed access to what resources. Endpoint Client security refers to checking the security status of desktop and notebook computers, or any device for which an employee is trying to establish a connection.

"Before the user's machine is allowed to connect, our SSL client checks to make sure it is properly secured," says WatchGuard's Scott Pinzon, editor-in-chief of the LiveSecurity Service. "It checks that the firewall, antivirus software and Intrusion Prevention System (IPS) are on and that you have antivirus updates. It can do a registry check and even check for keystroke loggers."

Using SonicWALL NetExtender VPN client plus the company's Enforced Client Anti-Virus and Anti-Spyware, IT administrators can set policies for a company-managed system, requiring that current antivirus and antispyware software be installed and active before the machines are allowed to connect.

Symantec Network Access Control "validates that the client coming in is up-to-date," says Tim Boyd, product marketing manager, mobile security group, at Symantec. For mobile devices and smartphones, Symantec offers Mobile AntiVirus for Windows Mobile and Mobile Security for Symbian. "You want as much automation as possible," Boyd says.

Trend Micro's Client Server Security for SMB will protect devices from viruses, spam, spyware, and other malicious threats, and requires zero administration. "We've made it easy to install, use and manage," says Jon Clay, product marketing manager, small and medium business segment, at Trend Micro. "We support POP3 (Post Office Protocol 3) e-mail scanning, so if your company is too small to use Microsoft Exchange, the client component can scan the messages."

Secure Log-in

The classic user ID/password is no longer considered sufficient for a secure login. Passwords can be guessed, stolen or cracked with "dictionary attacks" (decrypting passwords by trying a large number of possibilities — typically words found in a dictionary) or other tools.

"We also recommend a second authentication token," says WatchGuard's Nachreiner.

Biometrics — fingerprints, voice or palmprints — are becoming more popular as the second identifier. Vendors such as Hewlett-Packard and Lenovo offer business notebooks with built-in fingerprint readers; APC and IBM offer external USB (universal serial bus) fingerprint reader devices. USB flash storage drives include Lexar's JumpDrive TouchGuard, SanDisk Cruzer Profile and Sony Micro Vault with Fingerprint Access incorporates fingerprint-based access.

Currently, the most popular additional identifier, or token, is an additional alphanumeric sequence, generated fresh each time. The sequence generator can be credit-card-sized or a key-fob device, or a program in your computer such as RSA Security's SecureID.

"With an IPSec VPN, the user has to have the right software or configuration, or they can't connect," says John Masotta, senior manager, product marketing group, authentication products, at RSA Security. "But with SSL VPNs, someone can be at any system anywhere. So it becomes more important to confirm the identity of the user before permitting the connection."

RSA's SecureID solution provides two factors of identification: "something you know" — a memorized PIN code, and "something you have" — the code displayed on the SecureID smartcard, USB token or SecureID software for a notebook, mobile device or smartphone.

According to Masotta, more than 18 million people currently use SecureID — "mostly for securing remote access to systems."

Thanks to the RSA Secured program, SecureID works with, and can be easily added to, VPNs from most leading VPN vendors, including Cisco, Juniper Networks and SonicWALL. "We provide software they can build into their VPN, so when IT configures the VPN, the administrator can check the 'Use SecureID for authentication' box," says Masotta. "This makes it very easy for a company to install and use SecureID with their VPNs."

In fact, Masotta notes, many companies use SecureID to lock down access to company notebooks before users can even access programs and applications. "Once you've implemented SecureID, you can use it to lock down access to Web portals for e-mail Outlook access or to secure access to business applications on the network. If IT uses Microsoft Terminal Services or Citrix Presentation Server as an application platform when someone tries to access those applications, that platform will challenge them for their identity."

The RSA Authentication Manager, which validates the codes sent by users, is available for as few as 10 users, according to RSA's Masotta. Appliance versions of RSA's Authentication Manager can handle up to 50,000 users. ◊

Advice for IT

Ben Rothke, author of "Computer Security: 20 Things Every Employee Should Know" (McGraw-Hill, 2006):

"Read the regulations. You would be surprised how many people never even bother to read the text of the regulations they are expected to comply with."

"You can negotiate with regulators. Regulations are not black and white, and even though you may not be 100 percent compliant, if you have a plan to be, regulators can deal with that."

Attorney Daniel J. Langin, (specializing in compliance issues):

"There's a popular belief at the CXO level that technology security solutions should be a box or a piece of software. We forget that's only 40 to 50 percent; there are also policies, procedures, training and change management, which rely on technology but have to be used."

Robert Ayoub, industry analyst, Frost & Sullivan research firm:

"If you're providing connections to your corporate network, there needs to be some education on how employees can tell it's secure, that they're connecting over SSL, on a secure connection."

"People who are using secure sessions and two-factor authentication are, in general, meeting most of what you need to be compliant. The regulations are geared to 'Are you communicating securely?' 'Do you have two-factor authentication?' And 'are you running client-side antivirus, antispyware and firewall security software?'"

CDW offers technology service support from top manufacturers and service providers across all product categories.