



VISTA
The excruciating wait is over P. 28

E-EVIDENCE
Your compliance required P. 36

EMERGING TECH
Beyond passwords and biometrics P. 45

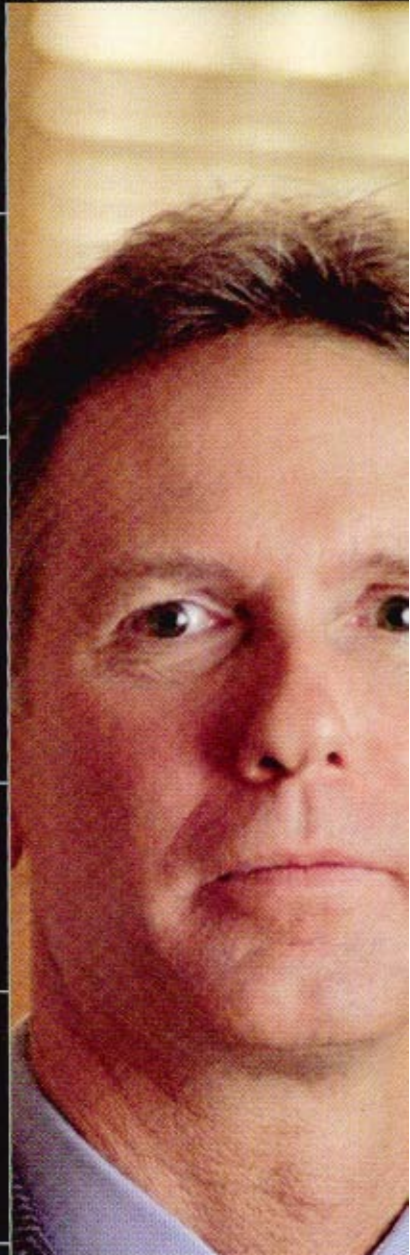
CHECKLIST
Ten steps to greater security P. 53

InformationWeek

DEC. 4, 2006 BUSINESS INNOVATION POWERED BY TECHNOLOGY



**WHO'S
UP TO
THE
TASK?**



Electronic records are critical to overhauling health care—the U.S. economy's No. 1 challenge

TECH PORTAL

SECURITY

Count To 10 And Be Secure

Don't get too comfortable—you may be ignoring these ways to keep your company safe

BEFORE YOU HUNKER DOWN in front of a crackling holiday fire, hold the fruitcake and eggnog: Feel like you're forgetting something?

Did you post a surveillance camera in your server room? Check the trash can for discarded disk drives that weren't wiped clean of sensitive data? Do a deep background check on that new database administrator?

Maybe you're not quite ready for the holidays. You're not alone. Most organizations have at least a few security issues that have been lost in the shuffle. So, as our contribution to your holiday shopping list, we've compiled this list of the 10 most overlooked aspects of IT security.

LOCK 'EM OUT

When you review your IT security architecture, you probably don't consider physical security. But that can be a lethal oversight.

"A lot of companies are allocating surveillance technology in the wrong places," says Steve Stasiukonis, VP and founder of Secure Network Technologies. Places where intruders are likely to gain access, such as the cargo landing where smokers take their breaks, often go ignored.

Leaving physical access to chance makes it that much easier for an attacker to simply walk in and make a network attack or other breach. Stasiukonis, who stages social engineering exploits to audit his clients' security, recently duped employees at a credit union client's facil-

ity, posing as a copier repairman stopping by to "clean" the copier machine.

"I busted in ... wearing one of those copier company T-shirts," he says. "I jacked in and grabbed the password and logins in clear text and then [used them] to break in from the outside, too."



Are You Paying Attention To These?

PHYSICAL SECURITY

PROPER DISPOSAL OF SENSITIVE DATA

BACKGROUND CHECKS

HOME COMPUTER USERS

BUILT-IN SECURITY

LOG FILE ANALYSIS

TRAINING

OUTSOURCING

ENCRYPTION

INTEGRATION OF SECURITY WITH SOFTWARE DEVELOPMENT

WATCH THE TRASH

Businesses dump tons of material on the curb, most of it useless landfill. But companies that don't have strong policies on garbage disposal may be leaving bits of gold for hackers seeking customer information or other sensitive data.

One of the most frequently overlooked treasures is the discarded hard drive. They're often sent to recycling centers or charities, or simply trashed with little, if any, attempt to wipe them clean of data. In a recent study, researchers at the United Kingdom's University of Glamorgan and Australia's Edith Cowan University bought more than 300 hard drives at auctions and computer fairs all over the world. They found an array of data that should have been erased, including payroll information, employee names and photos, IP addresses, and network information.

And companies shouldn't overlook one of the oldest forms of stolen data: paper trash. Jim Stickley, CTO at penetration testing company TraceSecurity, says he has found a wealth of sensitive information—including user identities and pass-

words—simply by going dumpster-diving.

FELON ALERT

It's easy to overlook the character issue when hiring employees. But as the strategic value of IT has risen, so has the need to ensure that those with the keys to the kingdom aren't eavesdropping, stealing, or worse.

Screening is now more the norm, says Jason Morris, president of Background Information Services. It's important to make sure there are no unexplained gaps in a candidate's job history, Morris says. Are they claiming Cisco router certifications? Confirm it. "Driver's records could also be a good measure of responsibility, as are credit reports."

How much should a company expect to spend on a background check? "A good rule of thumb is one day's salary" for the position for which you're hiring, Morris says.

OUT OF SIGHT, OUT OF MIND

Many IT groups carefully watch employees in the office, but they fail to monitor just what software users install or what hardware they plug into their PCs at home—or who else has access to those machines.

"The problem companies face with home workers is that the security boundary with the Internet has been extended to hundreds, even thousands of remote locations," says Geoff Bennett, director of product marketing at StreamShield. "The odds of a weak point are multiplied exponentially."

Top execs can be the weakest links in the home-user chain. "The CEO and CFO want to store sensitive data locally on their laptops because they don't want to worry about VPN-ing in," says Consilium1's Sean Kelly, a technology consultant who does penetration testing.



"In one instance, a CEO's kid got on his machine and renamed critical financial files," says Rob Enderle, principal analyst at the Enderle Group. "The firm was unable to do a planned stockholders' meeting as a result."

As home users increasingly become phishing and botnet targets, the company-issued laptop and the home PC with VPN access can leave the corporate network at risk. "If their machine has turned into a zombie and has access through a VPN to the corporation, the corporation is clearly exposed," Enderle says.

Companies can replace VPN access with biometric, multifactor authentication for e-mail, Enderle says. A home security audit and user training also are helpful.

OUT-OF-THE-BOX SECURITY

Security is big business these days. As a result, many vendors have begun to build security features into their hardware devices, giving them out-of-the-box capabilities that often go unused.

One of the best examples of this is the Trusted Computing Group's Trusted Platform Module 1.2, a set of specs that lets vendors add a security chip to any PC. Although most new PCs have TPM, many companies have yet to turn on the functionality, says Steven Sprague, president and CEO of Wave Systems. Businesses should turn on this technology and see what it can do, he says. "It'll change the way they look at end-user security."

KNOW YOUR LOGS

Log files aren't so much overlooked as unappreciated. Most IT and security pros have so much log

data that they typically only skim it, or ignore it altogether. But log files can be the key to recognizing an attack. External attackers typically use methodical approaches that can be identified in log trends. Internal attackers usually leave a clear audit trail in their logs that can be backtracked and exposed.

The trick is learning how to analyze log files in a way that's thorough but not too time-consuming. For most IT units, this means using a combination of automated log file analyzers, security information management tools, and detective work.

Many IT analysts analyze the logs but fail to normalize the data or study it for a long enough, says netForensics security strategist Anton Chuvakin. "To fully realize the value of log data, one has to take it to the next level of mining: actually discovering things of interest in log files without having any preconceived notion of 'what we need to find,'" he says. "That sounds obvious, but it's disregarded so often."

TIME FOR TRAINING

Some of the worst security problems originate from stupid things end users do—from the seemingly obvious one of opening attachments from strangers to connecting to the closest Wi-Fi connection while on the road. Training is critical, but often overlooked, element of security strategies.

The annual 60-minute security awareness training session, where you pack in everything your users need to know, isn't enough. "This is too much for the average user to absorb," says Todd Fitzgerald, system security officer for United Government Services. "More frequent security reminders are needed in a way



Computing Under Your Control

that is understood by the end user."

Training should be more "in your face" and "real," with posters, computer-based training, compliance tracking, and face-to-face interaction, Fitzgerald says.

OUTSIDE HELP

Some security pros believe the introduction of a third party to any phase of IT increases the risk of a breach. There's some truth to this, but experts say people who are too dogmatic about third-party services are overlooking an excellent way to increase security and save money.

Gartner had long been skeptical of third-party security services but reconsidered its position last year and began recommending that companies use outsourcing selectively.

In most cases, businesses are using outsourcers for labor-intensive tasks such as maintaining and upgrading firewalls or analyzing log files. This approach cuts the costs of handling these tasks while improving efficiency, experts say. Managed security services, in which providers offer a range of antivirus, anti-spyware, and intrusion-detection capabilities, are still popular in smaller businesses but haven't deeply penetrated larger companies.

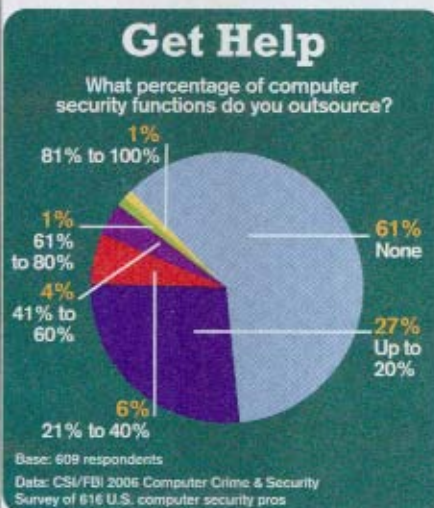
ENCRYPT SELECTIVELY

If encryption gets short shrift from IT, it's not because it's a low priority—it's because encryption can be complicated to manage. Questions about how to manage encryption keys, how to search encrypted archives, or where to deploy it persist. But many IT departments are being forced to deploy it by state and federal data privacy or long-term archiving regulations.

There's no need to blanket the enterprise with it. Pick your spots, experts say. Many IT groups have taken this to mean laptops and backup tapes—any place where data is portable and at risk. Others

also encrypt specific applications such as e-mail or business processes like payroll and benefits.

"It makes sense to encrypt anywhere there's material risk to data being stolen," says John Rotchford, managing director at Strategic Advisory Services International. "Laptops are a no-brainer but encrypting data at rest in a data center doesn't make as much sense, since the chances of someone ripping open a storage ar-



ray is probably pretty low."

Companies also need to consider how to bring intelligence into the equation. IT has to be able to manage encrypted data both in flight and at rest. And that means such data must remain easily searchable, which requires more forethought, says Eric Ogren, a security analyst with the Enterprise Strategy Group.

SECURE DEVELOPMENT

You can blame this one on software developers, but the onus is on the security organization to press them to build more secure software.

Even seemingly minor coding errors in software can cause big-time security headaches down the line for enterprises that deploy the buggy software. Many developers—both internal programmers and third parties—don't code their operating systems, applications,

and network device software with security in mind from the get-go.

Vulnerabilities and attacks would be less pervasive if developers had better processes for identifying coding problems and other bugs that lead to security woes. "There's not a lot of pressure [on vendors] to securely code things. Customers don't demand it," says Consilium1's Kelly. "Until organizations really start incorporating and integrating security into their development processes," there won't be much change, he says, although regulatory compliance demands are helping.

Microsoft is the most high-profile developer to embrace a secure coding with its Trustworthy Computing initiative, of which Windows Vista will be one of the first graduates.

"Because of Microsoft's position in the software product market as a platform provider, it's significant that they have launched a broad security initiative," says Robert Seacord, senior vulnerability analyst at CERT. Microsoft has already made one contribution: The ISO/IEC WG14 working group for the programming language C is developing standards based on a Microsoft library that remediates common programming errors, he says.

Meanwhile, enterprises must balance what features they need with security risks they can assume, Seacord says. Attackers will use the easiest route they can find, he adds. "If that attack vector can't be adequately defended because of other requirements, it makes little sense to expend significant resources eliminating one attack vector while leaving another vulnerable."

Secure coding is ultimately up to the developers, Seacord says. But IT and purchasing managers must make security a primary concern in their buying and design decisions.

—THE STAFF, DARK READING

Write to us at iweekletters@cmp.com