

## Seven Deadly Sins of Home Office Security

***Whether your home office is for the occasional WAH or you're running a business from the house, are you guilty of one of these security oversights?***

By [Joan Goodchild](#), Senior Editor

June 22, 2009 — [CSO](#) —

According to the human resources association World at Work, 17.2 million Americans worked from home or remotely at least one day per month for their employer last year. The 2007 book 'Microtrends' estimates that 4.2 million Americans work full-time from home.

Good security is a key to good productivity. CSO spoke with two home office security experts about security mistakes home office workers often make (and how to avoid those errors).

### ***1. Failing to physically secure the office***

Working out of a home in Southern Florida, Jeff Zbar knows all too well how important physical security is for his office. Zbar, a journalist, corporate copywriting and home office expert, runs the web site [chiefhomeofficer.com](#) and has also written several books, including "Safe @ Home: Seven Keys to Home Office Security."

During Florida's infamous hurricane season, Zbar has plywood ready to go for his office windows. He has storm shutters on them year round. But the physical security of his office goes far beyond weather concerns. His home also contains three children and three dogs, which can serve up a different kind of threat.

"These are things you've got to think about if your office is in the house. What if one of the children goes up and sees that pretty green light on the computer and they decide to touch it? What if they pull on the cable or the dog chews on the cables? I've made sure my computer is stashed in such a way they can't get to it when I am not around." Clearly, a lock on the office door itself may not be a bad idea.

Zbar also has fireproof lock boxes (Underwriters Labs (UL)-rated boxes are available at your local office-supply store) where he stores important documents and data in the event of a theft or disaster.

And consider a cross-cut shredder to help dispose of such documents when you're done with them.

### ***2. Failing to install the most basic computer security measures***

How much thought do people give to the security of their home office network?

"Most people typically go out and buy a router from Best Buy, throw it in there and call it a network," said Derek Krein, a wireless security expert. "It's pretty scary."

Krein, who is the chief technology officer with Advanced Wireless Networks in Virginia, says the assumption that home office networks are not common targets for criminals is dangerous.

"People think: 'I'm at home, no one is going to bother my home network,'" he said. "But by configuring the security properly, you make it difficult enough that criminals go elsewhere to find lower hanging fruit."

Krein's checklist for security layers includes: a network firewall and good [antivirus/anti-malware software](#), kept up-to-date.

He also recommends that those who have several computers in the home put a personal firewall on any laptop they are using to further protect it from infections that may have gotten into other computers in the home network. If your laptop has Windows XP, it comes with a personal firewall; all you have to do is enable it. Windows Vista has a firewall that is turned on by default. But if you're not working with a system that already has a personal firewall, software is available from most major security-software vendors.

### **3. Forgetting Wi-Fi security**

How many wireless networks can you log onto at home? Can you see your neighbor's network? Sure, you only log into your own. But can you trust everyone to be so ethical? How easily could someone get onto your network and see sensitive information?

Krein advises that home networks have some kind of encryption, such as Wi-Fi Protected Access, or the newer standard of encryption known as WPA2, enabled. It is important, said Krein, to ensure your wireless router is enabled and configured for encryption and that all wireless network devices are configured properly so the security will work. It takes some time, he said, but it is well worth it.

Most newer Wi-Fi-certified devices support WPA protocol; it is just a matter of configuring it properly to work, which is information you can probably get simply from the owner's manual of your wireless router. But if you are using an older device, you may need to upgrade.

### **4. Failing to separate your business from your home**

While it may not be necessary in all instances of home office scenarios, Krein recommends considering the nature of your work when deciding whether or not you need to segregate your work network from your home network. Certain types of work are subject to various laws and regulations. Using the same computer for work as you do for personal business could present an ethical, or even legal, issue."

"If you are doing work that requires [PCI compliance](#), such as working with credit card numbers, or if its medical work and you are bound by [HIPAA rules](#), you would want to segregate your networks."

And there is also the issue of letting family members onto the work computer, which is a mistake, said Zbar. It is a common scene for a child to use a home office computer when it isn't being utilized for business, but Zbar recommends against this.

"We have different computers with printers in the house for the kids for their school projects and other things," he said

The reason Zbar insists on separation is because of the lack of control he has over what his kids might do on the web.

"You don't want to make your computer more vulnerable than it needs to be by having others web surf on it and doing things with it."

Krein handles it a bit differently in his house. He has his computer set up for several users, with administrator privileges only under his own password protected profile. If children accidentally find themselves on a site with a malicious link, it would be much harder for them to download a virus or other malware, he said.

### **5. Failing to remember your office is a place of business and is held liable as such**

Zbar rarely sees clients or any other work-related individuals in his home office, preferring instead to meet them in public or at their place of business.

"For security purposes I think it's important not to have people in your home office," he said.

Zbar said he thinks it's safer not only from a security standpoint, but that there is a liability issue, too.

"What if you have someone to the office and they trip and fall?" Zbar said "I have insurance that covers me for some of that stuff, but I don't want to have to go through that."

## **6. Forgetting to back up data**

Ever had a sudden power outage and lost a few hours' work? Or worse, ever [fried a hard-drive and lost everything](#)? Data backups are a simple and necessary discipline.

There are many different ways to back up your data these days. Each one comes with a different price in terms of both money and time, said Krein. One obvious solution is to buy an external hard drive and keep to an appropriate schedule for manually backing up data. The danger with this plan, however, is that you may still lose information in the event of a system failure if you haven't manually backed up yet.

Other options include online storage services, network-attached storage, and disk imaging software. All are good backup technologies, said Krein. The most important point is simply to choose a solution and use it.

Krein also recommends having an uninterruptible power supply, or battery backup, in case of a power failure.

"With a battery backup ready to go, if you lose power, you'll still have time to continue to work and make sure you aren't losing anything," he said.

There are three kinds of UPS: standby, line interactive and online. They all provide battery backup, but they work in different ways. Figuring out which one you need depends on the kind of protection you require.

## **7. Failing to consider bigger business continuity issues**

If you work exclusively from home, your office is your world when it comes to your career. But many fail to consider the possibility of how to continue working if certain conditions, such as weather, or a fire, force one out of the house indefinitely.

Zbar is a vet in preparing for the worst because of his South Florida location.

"I always wonder what someone in Massachusetts or New York must think when I say, we have a storm coming, I might not be available for few days."

But these days, Zbar, who has worked from home since 1989, finds he rarely has to lose a day of productivity if a storm hits. Cloud computing gives him the ability to work from just about anywhere. However, those who have everything stored on a hard drive on a computer that has to be left at home may not be so lucky. Ditto for those who need to get their hands on sensitive documents that have no digital copy elsewhere.

"Everything you need on a day-to-day basis needs to be remembered if you are going to keep things running," said Zbar.

# **Criminal network to trade botnets and malware uncovered**

[Dan Kaplan](#)

June 17, 2009

Researchers at a web security firm have discovered what they term the latest milestone in the evolving cybercriminal underground: a one-stop-shop for hackers.

Called Golden Cash, the network enables cybercrooks to buy and sell control of compromised computers, as well as trade tools for creating malware and controlling and collecting data from botnets. Also, the platform contains about 100,000 stolen FTP credentials for sale.

The discovery of the Russian-based platform, believed to be run by individuals related to the Russian Business Network ([RBN](#)), was noted in the second issue of Finjan's [2009 Cybercrime Intelligence Report](#).

Finjan CTO Yuval Ben-Itzhak told SCMagazineUS.com on Wednesday that Golden Cash represents the next step in the professionalism of cybercrime markets. As a result of such platforms, people can expect attacks to grow in speed and efficiency, he said.

"It's no longer a big, technical effort [to conduct attacks]," Ben-Itzhak said. "This is the first time everything has been managed through the same interface. It's everything combined."

The going-rate to purchase packages of 1,000 compromised machines on the network ranges from \$5 to \$100, according to Finjan. Once the batches are bought, partners are then paid to distribute the botnet and collect FTP credentials entered on the victim PCs. Meanwhile, sellers can use the network to earn up to \$500 per 1,000 zombie computers.

Those running Golden Cash also have found ways to protect their operation, Ben-Itzhak said. For one, the platform blocks IP addresses belonging to security vendors (Finjan researchers used IP addresses not owned by the company). In addition, Golden Cash sits behind a number of proxy servers that hide the origin of the actual web server being used.

Gary Warner, director of research in computer forensics at the University of Alabama at Birmingham, said many in the investigative community have known about Golden Cash for some time, but this discovery helps spread the word about the slickness of the criminal underground.

"The news is that they've just been outed," Warner told SCMagazineUS.com on Wednesday. "Finjan has just exposed them to the public eye through their report. I would guess something will happen to them very quickly now that this has happened."

Finjan has notified law enforcement in Russia and Estonia. As of Sunday, the network still was operating, but Ben-Itzhak expects action to be taken soon.

He said businesses can do their part to lessen the success of such operations as Golden Cash by applying patches for vulnerabilities as they become available.

"When you leave these doors open, someone will come in your door," he said.

## Vinton Cerf: Outer Space Could be Next Frontier for Cybersecurity

[NextGov.com \(06/11/09\)](#) ; [Sternstein, Aliya](#)

NASA and Google Internet evangelist Vinton Cerf are currently testing an extraterrestrial Internet that could lead to technology for use in securing ad hoc networks during military operations. A decade ago, Cerf and NASA started developing an interplanetary Internet to regulate data transmission to and between devices in outer space. "This is moving ahead after a 10-year period of gestation," he says. "So, for me, this is like a science fiction dream that's finally coming true." Cerf, co-winner of the 2004 ACM Turing Award, recently said the technology being developed in that project could be applied to "terrestrial requirements." He says information security, shrinking user space on the Internet, and the lack of a system for monetizing digital information are key vulnerabilities that must be addressed by both the government and private industry. Cerf points to NASA's successful testing of interplanetary data transmissions in deep space and upcoming tests on the International Space Station. An interplanetary Internet needs to be more robust than the Internet infrastructure on Earth, and instead of relying on continuous end-to-end connections, each node on the network holds on to its information until it can safely communicate with another node, which prevents information from being lost when an immediate connection fails.

# The Ten Habits of Highly Secure Employees

## *Ten simple ways for employees to help protect company data and assets*

— [CSO](#) — You've decided to get away from your desk for lunch, but you've forgotten your access card. Since you only have a few minutes, you prop open a door. Seems harmless, right? Unfortunately, it's a move that creates some risks.

"Most company information isn't lost by electronic hacking, it's lost through individuals' mistakes or lack of knowledge of how to protect information," says Eddie Everett, senior vice president and national director of the global services department for risk consultancy Control Risks.

These 10 tips can help you avoid some common security blunders and give yourself, and your company, peace of mind.

- Be alert. Be aware. Challenge unknown people in the office—this can be done in a manner that is both direct and courteous. [Ask unaccompanied strangers wandering the halls where they are going and if they have a visitor ID](#). Someone who is supposed to be there won't mind the question.
- Prevent tailgating. We like to be polite, so we hold doors open for the people behind us, even if they're strangers. That's not a good practice to get into in any workplace area that requires authorized access. If you don't recognize the person following you through the door, ask for ID.
- Trust your gut. If something doesn't look right, it probably isn't.
- Remember the [clean desk policy](#). Conceal sensitive documents within your workspace, especially when you're working with confidential information.
- Secure your laptop while in the office. It takes a second for someone to snatch a laptop, and with it your company's intellectual property. Securing your laptop is much like locking your house—it's just a good habit.
- Don't [leave PDAs or thumb drives lying around](#). They're even easier to pick up than laptops.
- Don't assume that everyone who walks through your building is a friend of the company. If something looks wrong, get help.
- Be aware that other people will access open workspaces when you're not there. After hours, cleaners and maintenance workers come through. Plan accordingly.
- Keep quiet. If you're discussing sensitive issues regarding your company or clients, be sure only those you're conversing with can hear you. As Everett points out, "it's quite amazing what you can overhear in an elevator."
- And for those traveling on business—do you need all of the information you have in your briefcase? Probably not. Work on the assumption that you might lose what you're carrying, and make sure there is nothing on your laptop that is mission-critical to your company.

# 5 Ways to Strengthen FISMA

## Nation's IT Infrastructure at Risk, GAO Says

June 30, 2009 - Eric Chabrow, Managing Editor

The nation's federal and private-sector infrastructure systems remain at risk of not being adequately protected unless action is taken, the Government Accountability Office said in a letter issued Tuesday to a House panel.

"The need for improved cybersecurity in the federal government is clear," wrote Wilshusen GAO's information security issues director.

In the [letter](#), GAO offers five ways Congress can strengthen the Federal Information Security Management Act, the law that governs IT security in the federal government. The five proposals:

1. Clarify requirements for testing and evaluating security controls.
2. Require agency heads to provide an assurance statement on the overall adequacy and effectiveness of the agency's information security program.
3. Enhance independent annual evaluations.
4. Strengthen annual reporting mechanisms.
5. Strengthen OMB oversight of agency information security programs.

Wilshusen was responding to two follow-up questions by members of the House Committee on Oversight and Government Reform's Subcommittee on Government Management, Organization and Procurement, stemming from a May 19 hearing on federal information security. One question solicited the views of GAO, the investigative arm of Congress, on how FISMA could be improved; the other solicited GAO's view on the Cybersecurity Act of 2009, a bill sponsored by Senators Jay Rockefeller, D.-W.Va., and Olympia Snowe, R.-Maine.

Wilshusen says the bill, known as S. 773, is intended to improve cybersecurity in the United States. According to the bill, America's failure to protect cyberspace is one of the most urgent national security problems facing the country, a point Wilshusen didn't dispute. In the last fiscal year, he says, GAO determined that 23 of the government's top 24 agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. "The present cybersecurity strategy and its implementation had not been fully effective in mitigating the threat," he wrote. He reported that the number of IT security incidents reported by federal agencies has increased dramatically over the past three years, tripling from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008.

To remediate these problems, GAO recommended:

Developing a national strategy that clearly articulates strategic objectives, goals and priorities;

Establishing White House leadership;

Publicizing and raising awareness about the seriousness of the cyber security problem;

Focusing more actions on prioritizing assets, assessing vulnerabilities and reducing vulnerabilities than on developing additional plans;

Bolstering public/private partnerships through an improved value proposition and use of incentives;

Focusing greater attention on addressing the global aspects of cyberspace;

Placing greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts; and

Increasing the cadre of cyber security professionals.

"Until these improvements are considered," he wrote, "our nation's federal and private sector infrastructure systems remain at risk of not being adequately protected."

On the five ways to improve FISMA, Wilshusen wrote:

**Clarify requirements for testing and evaluating security controls:** "Federal agencies have not adequately designed and effectively implemented policies for periodically testing and evaluating information security controls. Clarifying or strengthening FISMA and its implementing guidance for determining the frequency, depth, and breadth of security control tests and evaluations could help agencies better assess the effectiveness of the controls protecting the information and systems supporting their programs, operations and assets."

**Require agency heads to provide an assurance statement on the overall adequacy and effectiveness of the agency's information security program.** "Such assurance statements should include an identification and analysis of significant deficiencies in information security, and should consider the impact of deficiencies identified in the agency's remedial action plans."

**Enhance independent annual evaluations.** FISMA be improved by specifically requiring that the independent evaluation be conducted in accordance with government auditing standards and include (1) an assessment of management's process for developing the conclusions in the assurance statement, (2) an identification of any significant deficiencies in management's process and (3) a statement about whether, based on the independent evaluation, there are any significant disagreements with management's conclusions on the overall adequacy and effectiveness of information security within the agency."

**Strengthen annual reporting mechanisms.** "(OMB) reporting instructions do not request inspectors general to provide information on the quality or effectiveness of agencies' processes for developing and maintaining inventories, providing specialized security training and monitoring contractors. In prior reports, we have also recommended that OMB develop additional performance metrics that measure the effectiveness of FISMA activities, such as requiring agencies to report on patch management and ensuring that all aspects of key FISMA requirements are reported on in the annual reports. We are currently reviewing the use of metrics to guide and monitor information security control activities at federal agencies and at leading nonfederal organizations."

**Strengthen OMB oversight of agency information security programs.** "OMB does not explicitly approve or disapprove agencies' information security programs. FISMA requires OMB to review agencies' information security programs at least annually, and approve or disapprove them. This mechanism for establishing accountability and holding agencies accountable for implementing effective security programs was not used. Implementation of this mechanism can provide additional oversight."

## New Information Security Controls to Strengthen Federal Cybersecurity Standards

Government Computer News (06/17/09) ; Kash, Wyatt

Federal cybersecurity standards should improve significantly this year for several reasons, according to Ron Ross with the National Institute of Standards and Technology (NIST). Ross cites several reasons for why he thinks federal cybersecurity standards will begin to improve, including NIST's recent rollout of an initiative focused on information security controls. That initiative is centered around NIST Special Publication 800-53, which attempts to harmonize the best information assurance and security practices and requirements across

civilian, military, and intelligence agencies. In addition, the publication provides a set of security priorities that federal agencies should adhere to. Ross says the initiative will have a major impact on the private sector because it would give "contractors a unified space" to work within. Another factor that Ross cites is a second strategic initiative from NIST that revolves around Special Publication 800-39. This publication provides a more comprehensive approach to managing enterprise risk and analyzing agency information systems' roles in the broader mission of agencies. Other cybersecurity experts say that a Senate bill that would bolster the Federal Information Security Management Act would also help to improve federal cybersecurity standards. That bill would force agencies to actively monitor and fix security flaws in computer systems and make agency officials more accountable for IT security problems.

## Guarding Networks

NextGov.com (06/25/09) ; Aitoro, Jill R.

Several high-profile security breaches during the past year have focused attention on federal chief information security officers (CISOs) and how they do their jobs. The increased attention has been welcomed by federal CISOs, some of whom say it has resulted in people beginning to understand what cybersecurity is, as well as what can happen when cybersecurity issues are not being addressed. That in turn has made the head of federal agencies more likely to heed the recommendations of their CISOs. However, a survey conducted by the International Information Systems Security Certification Consortium in the first quarter found that security managers believe they still need more resources and more support from senior management in order to achieve changing goals. Meanwhile, legislation being considered by Congress would make it more likely for CISOs to have their recommendations heard. Under the bill, called the Information and Communications Enhancement Act, CISOs would be required to report directly to the head of their agency instead of the CIO. Security experts are divided on whether the reporting change is beneficial or not. Some say CISOs should report to the agency head, who is responsible for ensuring information security is addressed in all agency initiatives. Others say it makes more sense for CISOs to report to the CIO because they can make sure information security is incorporated into IT projects from the beginning. In addition, those who favor having CISOs report to CIOs say the current arrangement is better because CIOs can ensure that security receives its rightful share of the agency's IT budget.

## Community Colleges Mobilize to Train Cybersecurity Workers

Chronicle of Higher Education (06/26/09) Vol. 55, No. 40, P. A17 ; Parry, Mark

Some experts project that the Obama administration's cybersecurity push will expand two-year colleges' role in supplying cybersecurity workers to government agencies, but among the challenges they must overcome is the struggle to train and hold onto qualified cybersecurity educators. Obama's proposed 2010 budget includes \$64 million in funding for the National Science Foundation's (NSF's) Advanced Technological Education program, whose projects include the establishment of a platform for cybersecurity education at community colleges. "The time is really ripe for community colleges' role in this area of technology to expand, be recognized, to get the kind of support that it needs," says NSF program director Corby Hovis. "All of the stars, I think, are aligned for this." Colleges are offering cybersecurity courses in anticipation that digital forensics and other cyberdefense areas will be a major source of future career opportunities. The NSF-supported CyberWatch consortium was established to build up the information-security workforce, and most of CyberWatch's 27 member colleges offer degree programs in technical assurance. One CyberWatch member, Anne Arundel Community College, developed a curriculum with National Security Agency representatives and other advisers that has been partially or completely adopted by nine colleges in the Washington, D.C., area. Consultant Daniel G. Wolf has advised companies to look to community college students for their cybersecurity needs, but University of Tulsa computer scientist Sujeet Shenoj says most community college cybersecurity education programs leave a lot to be desired.

# Survey Shows Widespread Concern About Mobile Device Security

Two-thirds of mobile phone owners are concerned about the security of their devices, concludes a study commissioned by device security vendor, Cloudmark. The survey, which polled 1,812 US adults who own mobile devices, shows that security concerns are preventing many users from adopting new mobile services for financial transactions and shopping. Meanwhile, mobile spam was also shown to be impacting a significant portion of mobile device owners.

Although new applications and services are rapidly emerging for mobile devices, survey results showed that users' perception of security is proving to be a significant barrier to their adoption, especially for mobile financial transactions.

Noteworthy findings include:

- 65 percent of all mobile device owners expressed concerns about the security of their device.
- Nearly half (46%) of these concerned device owners said that their worries about security prevented them from conducting activities on their mobile device.
- Of the activities mobile device owners said they were prevented from doing because of their concerns, financial transactions such as paying bills (73%), conducting banking activities (71%) and shopping (56%) were named most often.
- 79 percent of mobile device owners said that they have never sent or received confidential information of any kind through their device, which may further illustrate their lack of confidence in security.

The report also says that mobile operators also have a vested interest in supporting these offerings as an additional revenue stream. However, as convenient as these offerings are, the data from this study suggests that users may require additional assurance that mobile transactions can be conducted securely before they are willing to fully leverage these services.

Mobile device owners also indicated that mobile spam has established a highly visible presence on networks, with 44 percent of owners indicating that they have received spam on their mobile device.

"The prevalence of spam will only continue to rise as financial gain for spammers continues to increase," said Jamie de Guerre, CTO of Cloudmark. "For new services to succeed, it will be imperative for mobile operators to assure their customers of a secure environment for transactions, and to ensure that mobile spam does not impact the delivery of legitimate messages."

## Database Servers: Candy for Hackers

InformationWeek (06/20/09) ; Chickowski, Ericka

Enterprise databases, which often store confidential data that can easily be sold, are a favorite target of many hackers, according to a recent study by Verizon Business' computer forensics team. The study found that databases made up 30 percent of all the data compromises that took place in 2008. In addition, the study found that database breaches compromised three quarters of all records that were reported to have been breached last year. Since sensitive information is often stored in one company database, just one security breach can have serious repercussions. The Verizon study comes on the heels of other studies that also looked into database security. For instance, a recent study by Forrester Research found that database administrators spend less than 5 percent of their time on database security. Gartner's Jeffrey Wheatman said this is problematic because IT security personnel need the knowledge of database administrators in order to secure databases. Another recent study by the Independent Oracle Users Group found that many organizations take a long time to patch their databases. The study found that 26 percent of organizations take more than six months to install security patches on their Oracle databases, while 11 percent of organizations have never patched these systems. QuietMove's Adam Muntner noted that production databases often do not get patched as regularly as

they should because they are busy database servers and because people often do not see the reason for taking preventative security measures when there is no problem with the databases.

## **Report: No Magic Bullet for Database, Server Security**

**Dark Reading (06/11/09) ; Higgins, Kelly Jackson**

There is no easy way to secure data stored in databases and servers, and new technologies to protect against attacks on these systems are still many years away from being introduced, concludes a recent Forrester Research report. Co-author Jonathan Penn says protecting servers and databases has become increasingly difficult due to the introduction of cloud computing, the poor quality of the nation's job market, and the increase in the number of mobile users. He notes that while data classification technology could make it easier to protect servers and databases, it will not be ready for deployment until 2014, when security-specific data classification tools will be integrated with knowledge management and electronic records classification technologies. Another technology that could help protect servers and databases, data discovery technology, will not mature for several years, Penn says. As a result, organizations will have to rely on so-called brute force tools such as encryption and data masking to protect the information in their databases and servers until data discovery and classification technologies are ready to be deployed, the report says. The report also points out that organizations will continue to use database monitoring and Web filtering to detect breaches.

## **Women More Security Savvy, Vendor Finds**

**PC Advisor (06/20/09) ; Skinner, Carrie-Ann**

When it comes to cybersecurity, women are more diligent than men, finds a study by PC Tools. The security firm found that nearly 50 percent of men use the same passwords for online banking and vendors, compared with just over one in four women. Men have a more brazen approach to email attachments, with 60 percent confessing to viewing them immediately without checking first to see if they are safe, but less than 50 percent of women do the same. Conversely, most men understood the threats associated with online networking sites and email attachments, but nearly 50 percent of women were unaware that social networking sites can be dangerous. However, just 20 percent of men select the automatic update option on their security settings, and 30 percent of men admitted ignoring update warnings because they are "annoying." Roughly 40 percent of women adjust their security software to update automatically, according to PC Tools.

## **Feds Must Get Serious About Checking Commercial Software for Threats**

**NextGov.com (06/18/09) ; Aitoro, Jill R.**

During the past 10 years, federal agencies have increasingly chosen to purchase and install commercial off-the-shelf software instead of their own in-house applications. Although the use of commercial software has many advantages, there are a number of disadvantages as well. For instance, some commercial software programs are infested with viruses that can expose sensitive data stored on government networks, according to public and private sector cybersecurity experts. Among the experts warning of the threats that come with using commercial software is Mitchell Komaroff, the assistant secretary of Defense for networks and information integration and the director of the Pentagon's Globalization Task Force. He calls on agencies to address these threats by adopting life-cycle approaches that manage the full collection of risks. Komaroff notes that the Pentagon is doing its part by working with technology companies and the International Organization for Standardization to come up with guidelines that commercial companies can use to better manage risk. Meanwhile, consultant Gregory Garcia says federal agencies need to get assurances from the contractors and equipment vendors that the technology they are buying will not "phone home" or insert malicious code onto federal networks.

## Legit Websites Face Malware Hits

BBC News (06/17/09) ; Shiels, Maggie

Legitimate Internet sites are an expanding ground for malicious attacks with more than 10 million pages compromised annually. Security firm Dasient says the threat has increased as more people establish their own Web sites and blogs without adequate built-in security features. "This emerging threat is becoming very real and is already affecting millions and millions of Web sites," says Dasient co-founder Neil Daswani. "Thirty thousand Web pages are affected every day according to the likes of Microsoft and the security firm Sophos." Dasient says the emerging problem is not just attributed to inexperienced users or IT leaders who are being frugal on security. Modern Web technology is more sophisticated than in the past, increasing the exposures and the likelihood of attacks, a company official says.

## Administration Plans to Scale Back Real ID Law

Washington Post (06/14/09) P. A3 ; Hsu, Spencer S.

U.S. Secretary of Homeland Security Janet Napolitano is calling on lawmakers to change the Real ID Act to make it more palatable to states. Eleven states have refused to comply with the law because they say the federal government should be the one paying the \$4 billion cost of moving to more secure licenses. In an effort to get all states to comply with the law by the end of the year, Napolitano has asked the U.S. Senate to draft legislation that calls for the federal government to provide grants to states to help them rollout the new IDs. In addition, the new proposal--known as Pass ID--does not require the creation of new databases that would allow states to store and cross-check information such as information from federal immigration, Social Security, and State Department databases. The new proposal also eliminates the Real ID Act's requirement that motor vehicle departments verify the authenticity of birth certificates with the agencies that issued them. These requirements are replaced by stronger privacy controls. However, other elements of Real ID--including the requirement to use a digital photo, signature, and machine-readable features such as a bar code on the new licenses, and the requirement to verify driver's license applicants' identities and legal status by checking federal databases--remain in place. Supporters of Real ID criticized the changes, saying they will result in harm to national security. However, Real ID critics said the new proposal would still result in the creation of a national ID card.

## Do Web Applications Need Penetration Tests?

SearchSecurity.com (06/12/09) ; Cobb, Michael

Penetration testing is still necessary to verify the security of Web applications, despite improvements in the security software development process. The Payment Card Industry Data Security Standard requirement 11.3 still requires internal and external penetration testing on networks and applications on an annual basis. Penetration testing is still highly regarded by security professionals in Europe and North America as a sound method of detecting vulnerabilities and defects present in even the most scrutinized applications. For example, third-party penetration testing of government networks in the United Kingdom became a key requirement of gauging protections against external attacks after the 2008 Data Handling Review of security protocols in the region.

## Apple Working on Patch for iPhone SMS Vulnerability

(July 2, 2009) Apple computer is reportedly working on a fix for a vulnerability in the way iPhones parse text messages received through SMS, or Short Message Service. While the details of the flaw have not been released, it could be exploited to install and execute arbitrary code remotely. This means attackers could determine the location of the phone with GPS, turn on the phone's microphone feature, or recruit the device into a botnet.

Apple expects to release a fix for the flaw before the Black Hat Security Conference later this month, where additional details about the vulnerability will be discussed.

[Editor's Note Skoudis): **This is a big concern, because the iPhone and other smart phones are the ultimate spying devices. If I compromise your phone, I can get real-time updates on where you are (via GPS), the sounds around you (the microphone), what your phone can see (the still or video camera),**

whether you are walking (the accelerometer), your recent e-mails, your contacts... In a sense, you are completely owned, in a more privacy-invasive fashion than occurs with the compromise of your PC.

## Kentucky County Government bank Account Targeted by Internet Thieves

(July 1, 2009) Hackers are believed to have stolen more than US \$400,000 from the bank account of Bullitt County, Kentucky. The intruders gained access to the Bullitt County computer network with a stolen user name and password, and transferred the funds out of the county's account and into other accounts around the country. US \$45,000 has been recovered. The attackers are believed to be based in the Ukraine and have cohorts in the US. An undisclosed source says the cyber thieves used the Zbot Trojan Horse program in their attack. The malware allowed the attackers not only to steal login information, but also to connect to the bank through the user's own connection, so the session would not look suspicious to the bank.

[Editor's Note (Skoudis): I remember the debates of a couple of years ago, when we wondered when cyber crime cases and thefts would exceed non-cyber cases. Now, I'm wondering why any thief even bothers with non-cyber cases at all.]

## Solving the DLP Puzzle: 5 Technologies That Will Help

By Bill Brenner

July 8, 2009 02:51 PM ET

*CSO - About this series: Companies are clamoring for Data Loss Prevention (DLP) tools to keep their data safe from online predators. But there is much confusion over what the true ingredients are. In this series, [CSOonline](#) talks to security practitioners, analysts and other experts for a crash-course on what DLP is, what it isn't and how to get on the right track. We'll begin with the proper technologies to use, followed by the right people policies.*

Most security vendors will tell you they have just the thing for your DLP needs. But some industry experts say enterprises often buy products that, once installed, don't perform all the functions necessary to keep sensitive information safe.

We reached out to several IT security professionals in an effort to zero in on the true elements of an effective DLP program -- from the technology to people policies -- and how best to fit the pieces together. This article will focus specifically on five technological approaches that, when used together, offer a solid data defense.

[See also: Data Loss Prevention Dos and Don'ts](#)

### 1. Data discovery, classification and fingerprinting

Richard Stienon, chief research analyst at IT-Harvest, said a complete DLP solution must be able to identify your IP and make it possible to detect when it is "leaking."

William Pfeifer, CISSP and IT security consultant at the Enforcement Support Agency in San Diego, agrees, calling data classification the prerequisite for everything that follows. "You cannot protect everything," he said. "Therefore methodology, technology, policy and training is involved in this stage to isolate the asset (or assets) that one is protecting and then making that asset the focus of the protection."

Nick Selby, former research director for enterprise security at The 451 Group and CEO/co-founder of Cambridge Infosec Associates, said the key is to develop a data classification system that has a fighting chance of working. To that end, lumping data into too few or too many buckets is a recipe for failure.

"The magic number tends to be three or four buckets -- public, internal use only, classified, and so on," he said.

### 2. Encryption

This is a tricky one, as some security pros will tell you encryption does not equal DLP. And that's true to a point.

As former Gartner analyst and Securosis founder Rich Mogull put it, [encryption is often sold as a DLP product, but it doesn't do the entire job by itself](#).

Those polled don't disagree with that statement. But they do believe encryption is a necessary part of DLP. "The only thing [encryption doesn't cover] is taking screen shots and printing them out or smuggling them out on a thumb drive. Not sure I have a solution to that one. It also leaves out stereography, but then is anyone really worried about that?" Pfeifer asked. Specifically, he cites encryption as a DLP staple for protecting data at rest, in use and in motion.

Stiennon said that while all encryption vendors are not DLP vendors, applying encryption is a critical component to DLP. "It could be as simple as enforcing a policy," he said. "When you see spreadsheets as attachments, encrypt them."

### 3. Gateway detection and blocking.

This one would seem obvious, since an IT shop can't prevent data loss without deploying tools that can detect and block malicious activity.

Sean Steele, senior security consultant at InfoLock Technologies, said the key is to have something in place that provides real-time (or close to real-time) monitoring and blocking capabilities for data that's headed outbound at the network perimeter, data at rest ("sensitive or interesting/frightening data sitting on my network file shares, SAN, tier 1/2 storage, etc.," he said); and data being used by human beings at the network's endpoints and servers.

### 4. E-mail integration

Since e-mail is an easy target for data thieves, whether they are sending e-mails with links to computer-hijacking malware [see [Botnets: 4 Reasons It's Getting Harder to Find and Fight Them](#)] or sending out e-mails from the inside with proprietary company data [see [Embarrassing Insider Jobs Highlight Security, Privacy Holes](#)], partnerships between security vendors and e-mail gateway providers are an essential piece of the DLP puzzle. Fortunately, Stiennon said, "Most DLP vendors formed partnerships with e-mail gateways early on."

### 5. Device management

Given the mobility of workers and their computing devices these days [laptops, smart phones, USB sticks], security tools that help the IT shop control what can and can't be done with mobile devices is a key ingredient of DLP.

Stiennon is particularly concerned about the [USB devices that could be used to steal data](#). "Being able to control the use of USB devices is a key requirement of a DLP solution," he said.

## Text message scammers quietly prey on regional banks

**By Robert McMillan**

July 10, 2009 05:07 AM ET

IDG News Service - You get a text message from your bank telling you there's been suspicious activity on your account. You call the number on your phone to see what's going on, and before you know it, you're a victim.

Welcome to the next big thing in phishing.

Law enforcement and security experts say that for more than a year now, scammers have been using scam text messages to prey on small regional banks and their customers. And according to a [report](#) set to be released next Tuesday by Cisco Systems, the problem has only been getting worse in recent months.

"It's a serious problem," said Pat Peterson, a security researcher with Cisco.

Here's how the scam works. The criminals pick a bank -- say a credit union in Medford, Oregon -- then they bombard every phone in Medford's 541 area code with a phishing message sent by SMS (Short Message Service) telling the victims to call a fake 800 number that looks like it's from a local credit union. Because they're

targeting a bank in the region, the bad guys have a pretty good chance of hitting real customers who may not have heard about the scam.

They use the open-source asterisk software to set up a fake voice-operated system and steal information when people enter their account numbers, passwords and other sensitive information to authenticate themselves on the system. When the criminals use this information to transfer money overseas, the banks take the loss.

By targeting regional banks, the scam has managed to stay somewhat under the radar and not attract a lot of attention, said Nick Newman, a computer crimes specialist with the National White Collar Crime Center. Big banks have large security teams set up to tackle this type of fraud, but with a regional institution such as a credit union, "their entire IT team for the bank might be only five people," he said.

Another problem for the banks is that the scam subverts one of the main techniques that banks and security experts have been trying to drill into their customer's heads for years now, Newman said. "We always say, 'If you have any questions, call your bank, or they'll call you.' Well SMS is pretty close to calling your bank. It gets to the point where it's like, 'What do we tell people to do now?'"

This past weekend, the scam hit southern California, where [Wescom Credit Union](#) and [Farmer's & Merchants Bank](#) were targeted. But they're just the latest of many.

The criminals have been going through the country credit union by credit union, bank by bank, Peterson said.

"It's working pretty well for them," he added. "It's a pretty innovative technique."

Sometimes it works exceptionally well, in fact. When Medford's [Bank of the Cascades](#) was hit with the attack in May this year, the scammers got more than they bargained for, according to Detective Sergeant Kevin Walruff with the Medford Police Department. "I've spoken with people that gave their personal information and aren't even customers with Cascades bank," he said. "They actually called that number and provided information."

## Cloud storage triggers security worries

IT managers are charmed by the concept but fear giving up control of data.

Here's why.

By Robert L. Mitchell

July 13, 2009 12:01 AM ET

Computerworld - Liz Devereux knows a thing or two about cloud storage. As director of IT storage and digital imaging at Banner Health, Devereux oversaw the construction of an internal 150TB storage grid. The grid delivers storage as a service to the Phoenix-based health care provider's network of hospitals and health care facilities in seven states, which use it as a repository for radiological images. But she would never [entrust that data to an external cloud service provider](#).

"I'm nervous about someone else controlling my data," Devereux says.

Cloud storage offers some enticing advantages. It's pay as you go, with no capital outlay and no need to buy extra equipment in anticipation of future storage demands. You scale storage dynamically and pay only for what you use. But you must [trust your data to the cloud](#) -- and the vendor behind the service.

Few midsize or large businesses are willing to trust the cloud today, although some are experimenting. "There's a huge amount of interest," says Gene Ruth, an analyst at Burton Group. But, he adds, none of his firm's Fortune 100 clients is using a cloud storage service for live data today.

It's probably wise to proceed with caution, says [James Damoulakis](#), chief technology officer at Glasshouse Technologies Inc., an independent IT consulting and services firm that focuses on enterprise data centers,

storage and other elements of the IT infrastructure. "Cloud storage today is pretty much an early-stage concept," he says.

Aside from a few heavyweights, like [Amazon.com Inc.'s Simple Storage Service \(S3\)](#) and Verizon Communications Inc.'s Online Backup and Restore service, most offerings come from small start-ups. "It's best suited for low-priority or low-access, low-touch kinds of applications, primarily file-based as opposed to block-based," says Damoulakis, who is a *Computerworld* columnist. But he says he does have clients that use services from Amazon as temporary expansion space for testbeds or marketing programs.

Joe Mildenhall, CIO at Apollo Group Inc., is taking baby steps into cloud storage. "We have a lot to lose. If we're playing, we're only going to play with the big guys," he says. The Phoenix-based for-profit educational institution is using Amazon's S3 to temporarily store papers that some of its 400,000 college students submit through the Apollo Web site.

But even with Amazon, Mildenhall will entrust only low-risk data to the cloud. For example, students can submit Word documents to the Apollo Web site, which runs the documents through a grammar-checking engine and then parks them in Amazon's S3 storage. When a student retrieves his document, the data is purged. "The major characteristic is that it's not very important storage to us," Mildenhall says.

So far, the integration with S3 has worked well. But Mildenhall is still wary. "If [Amazon went down](#) for two days, my opinion would change," he says.

## Feelings of Insecurity

The most common storage-as-a-service offerings are online backup and archiving applications. Things have changed since the days of StorageNetworks, a company that couldn't make a go of hosted backup and closed its doors in 2003. The original idea behind StorageNetworks was outsourcing -- providing a service that used the same storage frames that were in the data center, says Damoulakis. Now, many cloud storage services use low-cost, commodity storage in a distributed architecture. "We've advanced very far in virtualization, the Internet, distributed computing and the grid concept," he says.

Michael Peterson, president of Strategic Research Corp., launched a storage service provider in those early years and was a business and technology adviser to StorageNetworks. He says *cloud storage* is a very broad term that incorporates a variety of technologies and business models. For example, some service providers use distributed, commodity storage, while others might use traditional midrange or high-end storage frames. That means that it's important to understand what you're buying.

But there is a common theme: [virtualization](#). "[Cloud storage] includes everything and is a virtualization model," Peterson says. Cloud is a catalyst for change, not a technology, and as such, it will bring about broader use of virtualized practices, he predicts.

Cloud storage service offerings range from basic file-based storage infrastructure services, like Amazon's S3, all the way up to storage-as-a-service applications. With the exception of start-up Zetta Inc., most vendors aren't pitching the cloud for primary storage.

In the business market, remote backup has always been the real driver for cloud storage, Peterson says. Nonetheless, most large businesses remain on the sidelines.

One of the biggest concerns IT organizations have with cloud storage is data security. Many cloud storage vendors offer encryption for data in transit and at rest. Some, such as Zetta, make encryption the default setting. That's important because in a storage cloud, your data might be on the same disks as data from other users, says Ruth. If another customer's data is raided by the FBI, for example, could yours go with it? "The laws are not sufficient to protect innocent parties whose data is on the same equipment," says Ruth. To address that, some vendors keep each customer's data on a separate disk. Zetta encrypts each customer's data with a different key.

Mildenhall says he feels confident that Amazon will be around for a while, but he still doesn't trust that the data will be. If he were to entrust business data to Amazon's storage service, he says he would need a mechanism to

ensure that a copy of the data was replicated back to his data center. "I'm not willing to say that the copy of data in the cloud is the only copy I've got," Mildenhall says.

Fear of vendor lock-in is another concern. Every storage service provider has its own proprietary APIs. In some situations, the user might also want to define metadata associated with a data set, such as aging information or security parameters. But storage service providers handle that differently as well, says Ruth. "These services shouldn't require specially designed interfaces to make them work," he says. Vendors are just starting to work on standards to eliminate the problem.

The lack of common APIs would create problems if a storage service provider were to suddenly shut its doors -- and that's a possibility when you're dealing with a start-up. "Once you get in bed with a service provider, you hope to heck they're not going to go out of business," Ruth says.

It's not how to get the data back that worries Manjit Singh, but whether he'd even have access to the data if the provider went belly up. "If it's bankrupt, the creditors might just come in and take the equipment, and they don't care what's on it," says Singh, vice president and CIO at Chiquita Brands International. He has yet to give cloud storage a try.

Rich Zoch is experimenting with Zetta's storage service at the University of Texas at Austin -- but not for primary storage. "It's a great platform to offload backup archives that are encrypted," says Zoch, senior systems administrator. But so far he has trusted the service only with dummy data. He says he plans to use it as a secondary storage pool for backups as an alternative to tape.

Zoch says he likes the fact that Zetta uses public key encryption that's compliant with Federal Information Processing Standard 140-2, but the university still might decide to encrypt the data itself before transmitting it. And since he's using Zetta only for secondary copies, he's not worried about getting it back if something happens on Zetta's end.

It might also be impractical to move large amounts of data from a cloud storage provider's site if the communications pipeline is too small. "If you can do only 1MB/sec. or 2MB/sec., it could take months or even years to get your data back," says Jeff Treuhaft, co-founder and CEO of Zetta. He says putting in a dedicated connection capable of transferring data in a timely fashion adds about 25% to the cost of Zetta's service.

Even if the stored data is accessible, some storage-as-a-service applications, such as Zmanda Inc.'s backup and recovery systems, store data on a third-party platform such as S3 on the back end. So it's important to do due diligence on where and how data is hosted and how to get it back, says Singh. But, he says, that's no different from the checks one should do with any other software-as-a-service provider that stores data.

What's the best way to get started with external cloud storage services? "You have to trust, but verify," Ruth says. That means touring the data center to see what's stored where, creating a service-level agreement with meaningful metrics and performing regular audits to make sure the vendor is living up to them. And if the storage-as-a-service provider is using a third party for the underlying storage infrastructure, you'll need to perform due diligence on that vendor as well.

Despite the challenges, most users see a bright future for cloud storage. Singh says he could see a role for cloud storage for file services if he had to replace his file servers. Others see the cloud as a potential way to back up remote offices.

Mildenhall says he sees a larger role for cloud storage at Apollo as well. "It would be reasonable to put file sharing and e-mail in the cloud," he says. And Mildenhall says he envisions a day when core business data might be hosted in the cloud -- as long as he has backups of everything.

Ultimately, Ruth says, IT organizations might use cloud storage as an alternative to building additional data centers to hold copies of critical information. But, he adds, "they need to get over the idea of moving the data off-site."

