

Security Trends Report

01/08

Malware evolving too fast for antivirus apps

But since you've got to live in the world regardless, a few tips

Erik Larkin

January 01, 2008 (IDG News Service) -- If you think that the latest security suites afford complete protection against malware attacks, think again. Today's for-profit malware pushers use dedicated test labs and other increasingly professional techniques to improve their chances of infecting your computer. And the techniques they employ to outpace security software makers appear to be working.

Make no mistake -- a good security program can go a long way toward keeping you in control of your system. But [PC World's](#) recent tests of security suites found that new malware easily evaded the applications. In our tests of how well security software blocks unknown malicious programs, the best performer detected only one in four new malware samples. In contrast, February 2007 results from similar heuristics testing showed that the best utilities caught about half of new samples.

Window of opportunity open

"In this industry, unlike others, we have an antagonist we have to deal with, someone we're constantly battling back and forth with," says Hiep Dang, director of antimalware research with [McAfee's Avert Labs](#). "The bad guys have the element of surprise."

Even just a 12-hour head start can translate into thousands of infected PCs, and malware authors have long tested their programs against antivirus applications to make sure they get that critical jump on the opposition. VirusTotal.com and similar Web sites, which allow security researchers and consumers to submit a questionable file and have it scanned by more than 30 different antivirus engines, have unfortunately made the testing easier for malware writers: Crooks can continue to tweak their new malware projects until VirusTotal or one of the other new multilanguage sites shows that the rogue application can slip past the majority of antivirus programs.

Good vs. evil?

Bad guys' use of sites such as VirusTotal can have a hidden benefit. After online thugs submit a sample, VirusTotal can sometimes share it with security companies, which can then update their programs to block the new malware. But the site permits users to opt out of having their samples submitted to antivirus vendors.

VirusTotal says it offers the option so that people can scan sensitive files at the site without having them broadcast to companies.

Some well-organized criminal groups go a step farther and "maintain their own antivirus setups, almost like their own VirusTotal," according to [Don Jackson](#), senior security researcher with the security services firm [SecureWorks](#).

Keep your guard up

Jackson says the opportunities for prerelease testing make for harder-to-catch malware--and underscore why smart PC users should never assume that their machines are immune to attack. For example, almost every day, SecureWorks sees new variants of the PRG Trojan horse made with a particular kit. And when the new versions first appear, usually only 25 percent of antivirus scanners detect them, he says.

As bad as all of that might seem, don't throw in the towel and resign yourself to the inevitability of infection. For one thing, antivirus programs can do very well once their creators learn about a new sample. When fully updated and pitted against PC World partner AV-Test's "zoo" of 675,000 Trojan horses, keyloggers, and other malware, the best-performing security suites detected 98 percent of them.

And security companies are aware of the challenge they face in keeping pace with nimble online thieves. McAfee and [Symantec](#) are focusing on additional layers of security, including firewalls and behavioral scanners, which detect malicious software based on its behavior rather than on a signature match.

Join the good fight

Multilayered security is important, but you are the most important component by far. AV-Test's results (and other security analyses) show that no program can provide complete protection. Some malicious and creative entrepreneur will always discover a way around any particular security program.

Getting around you can be much harder for malware creators, however, if you follow basic precautions. Crooks are quick to pounce on fresh program vulnerabilities, so be sure to keep all of your applications -- not just your Web browser and Windows -- up-to-date to seal off entire avenues of attack. Also, the best social-engineering tactics often accompany the newest and hardest-to-detect malware. If you assume that every unexpected e-mail attachment is an attack, and ask for confirmation from the sender before opening any attachment, you'll block another huge chunk of potential infections.

Malware authors may obtain a temporary lead over antivirus programs, but if you take sensible precautions in addition to running security tools, they won't get a leg up on you.

"Identity Theft in 2007, Predictions for 2008"

Government Technology (12/19/07)

The Identity Theft Resource Center has released its annual report, which reviews the identity theft trends of 2007 and anticipates the crime's developments in 2008. Researchers found that identity thieves are increasingly counterfeiting new checks and stealing existing checks in response to credit issuers' new, more stringent authentication policies. Web sites that sponsor online auctions and social networking remain a target for thieves. Conventional scams, such as lotteries, and domestic identity theft continue to thrive as well. Identity theft has also developed a symbiotic relationship with other crimes to fund and expand lucrative crimes such as drugs and terrorism. Nevertheless, companies, law enforcement, and consumers have achieved improved communication regarding the sources of identity theft and strategies for decreasing such crimes. Many are also recognizing that identity theft can be criminal in nature, as identity thieves can use a victim's Social Security to obtain employment or to collect welfare. ITRC's forecast for identity theft in 2008 includes the observation that identity theft is developing into a profitable career path and is becoming more global in scope. As thieves grow more skilled, scams will become harder to spot. Experts also predict a rise in the number of data breaches caused by weak data management policies. However, ITRC also anticipates that companies will create improved strategies for verifying applicants' identities, that law enforcement will increasingly categorize identity theft as a crime, that new legislation will aim to curb identity theft, such as by restricting the use of Social Security numbers, and that states and organizations will be better able to offer victims assistance for free.

"DHS Puts Cybersecurity Toward Top of 2008 To-Do List"

Federal Computer Week (12/13/07) ; Bain, Ben

In his year-end remarks, Department of Homeland Security (DHS) Secretary Michael Chertoff announced that cybersecurity will be one area of DHS' four key areas of focus in 2008. Indeed, DHS and Congress are collaborating to design a cybersecurity model that Chertoff envisions as the template for the next 10 years regarding how the United States handles the growing cybersecurity threat. Chertoff says this emphasis on cybersecurity is driven by the realization that much of the nation's economic health "depends on our ability to use the Internet and to use data systems in order to perform our work." Secure identification, immigration and border security, and a push to "institutionalize" the agency's operations are the other areas slated to receive heightened attention in 2008. However, many lawmakers were disappointed that DHS did not classify public safety interoperable communication efforts, including fusion centers and information sharing programs, as a vital area of focus for 2008.

"Managing Technology 2008"

Government Executive (12/01/07) Vol. 39, No. 21, P. 32 ; Aitoro, Jill R.

Securing personal information for both the public and for government workers will be a key aspect of data security in 2008, according to feedback from IT managers, researchers, and consultants. Indeed, as of October 2007, personally identifiable data was exposed in 30 incidents a day, on average, according to reports from federal agencies. Organizations are striving to prove that they know how to respond to a privacy breach; response guidelines can be found in past laws and communications. The Homeland Security Department recently updated the 1974 Privacy Act to mandate every agency to ratify rules of conduct for employees working with records systems, and to institute technical, physical, and administrative defenses to guarantee records' confidentiality. The Office of Management and Budget also published memorandums on privacy that compel every agency to appoint a senior agency official for privacy and to review all policies and processes. Agencies are also required to report all security incidents that expose personally identifiable information to the U.S. Computer Emergency Readiness Team within one hour of the incident. To reduce risk, agencies should treat personal information the same way they treat other sensitive data, particularly when kept on mobile devices. Experts add that 2008

would be a good time to ensure that agencies are using the National Institute of Standards and Technology's checklist, which includes such tasks as encrypting all data and locking applications housing personal information.

Visa Card Issuers Accept TJX Settlement Offer

(December 18 & 20, 2007) New England banks and other financial institutions that issue Visa cards have agreed to accept the US \$41 million reimbursement offer from TJX Cos. to cover costs incurred when they had to notify customers of the data breach and reissue cards. The proposal required 80 percent agreement to pass. The banks will receive their share of the funds within one week. In turn, they will dismiss all claims against TJX.

More Executives Say Information Security Can Improve Efficiencies, Drive Business Results

Dec 21, 2007

New research from Ernst & Young indicates that companies are having trouble balancing the traditional risk mitigation aspect of information security with its role in improving business performance.

By Katherine Walsh

Ernst & Young's 10th annual Global Information Security Survey shows promising evidence that a growing number of organizations believe information security can improve overall corporate performance, as well as protect corporate assets.

However the survey, which canvassed 1,300 senior executives in more than 50 countries, also shows that companies are struggling to strike a balance between performance initiatives and risk mitigation strategies.

According to the study, "Information security teams must connect with executive management and be involved with the strategic decision-making process from the beginning. This alignment has a positive impact on the bottom line and elevates information security from a technology deployment function to a strategic imperative."

Key findings:

* Eighty-two percent of respondents reported some level of information security integration with overall organizational risk management, and 29 percent report full integration.

* Sixty-nine percent of respondents said that information security improves IT and operational efficiencies. (In the past, information security has been viewed as a barrier to IT and operational efficiency.)

* Fifty-eight percent of this year's respondents said privacy and data protection are the second and third most important drivers behind infosec improvements, up from 41 percent in 2006.

* Although 64 percent of respondents ranked compliance as the primary driver of improvements to information security, 45 percent ranked meeting business objectives among the top drivers.

However, information security is still too isolated from executive management and the strategic decision-making process. Thirty-two percent of respondents rarely meet with their board or audit committee. While involvement is increasing, it continues at a slow pace.

More than 50 percent of respondents say that the number one challenge to delivering information security projects is a lack of experienced resources. To that end, 60 percent say they are outsourcing certain aspects of information security.

Monetary Loss From Phishing Attacks on the Rise

Jan 02, 2008

An estimated 3.6 million people in the United States lost money through phishing attacks between August 2006 and August 2007, according to new research from Gartner. That's a considerable increase from the 2.3 billion who lost money through phishing the year before.

The average dollar loss per incident declined from \$1,244 in 2006 to \$886 in 2007, but because there were more victims, more money was lost to phishing in 2007. In all, phishing attacks cost U.S. adults \$3.2 billion in 2007, according to the study, which surveyed more than 4,500 online adults.

Other findings include:

* Thieves are increasingly stealing debit card and other bank account credentials to rob accounts. According to the survey, 47 percent of consumers who lost money to phishing attacks said they had used a debit or check card as the payment method when they lost money or had unauthorized charges made on their accounts. Thirty-two percent of respondents said they used a credit card as the payment method, and 24 percent used a bank account to pay.

* The amount that consumers were able to recover increased. An estimated 1.6 million people recovered 64 percent of their losses in 2007, up from the 54 percent recovered by 1.5 million adults in 2006.

Avivah Litan, a Gartner analyst, says the increase in monetary losses from phishing attacks is partially due to the fact that many consumers aren't properly protecting themselves. Eleven percent of online adults say they don't use security software (antivirus or anti-spyware products) on their desktops. Forty-five percent only use what they can get for free.

Gartner says that although consumers need to be aware of phishing risks and protect themselves from attacks, e-mail providers, advertising web sites and other "infection point" providers need to take some responsibility, too. Providers need incentives to keep phishing e-mails from reaching consumers at all, and advertisers need to stop malware from being put on their websites.

"Enterprises should at least protect their own brands from being used in phishing attacks by subscribing to an anti-phishing solution," said Litan in a Gartner press release. "Similarly, companies should subscribe to anti-malware services that detect malware targeting the firm's customers, and prevent it from spreading across consumer desktops."

E-discovery Rules Still Causing IT Headaches

Many say the new archiving guidelines fail to account for evolving technologies.

Brian Fonseca

January 07, 2008 ([Computerworld](#)) -- Many IT shops have spent months working to refit corporate systems so they comply with year-old changes to the Federal Rules of Civil Procedure, even as some executives say the revisions aren't clearly defined.

However, some IT executives who complained about the rules did acknowledge that the FRCP modifications have forced them to make positive changes to corporate data-retention policies.

The revisions, which took effect on Dec. 1, 2006, require that opposing sides in a federal lawsuit meet within 99 days of its filing to determine what electronic data must be produced and in what format. Failure to comply could lead to fines or a prison sentence.

The e-discovery rules have been created and are enforced by the U.S. Supreme Court and are often followed in state courts as well.

IT staffers at Webcor Builders Inc. have been struggling to understand the ambiguous rules while simultaneously working to determine where all relevant data resides and how it can be accessed quickly in case of litigation.

Gregg Davis, CIO at the San Mateo, Calif.-based construction firm, contended that the rules fail to take into account evolving storage technologies.

"The new rules require that electronic data be in its native format," he said. "This is easy to achieve when it comes to e-mail, which was the provision's main target. But it gets very murky when it comes to propriety databases and homegrown applications.

"There are still a lot of questions around what is digital storage and e-discovery," Davis added. "The [revised] rules have changed the game, and we are [being forced to] think and rethink where things are stored."

For example, he noted that Webcor still isn't sure whether images and documents on copy machine hard drives and print servers fall under the revised guidelines.

The latest revisions prompted Webcor to re-evaluate its overall data- retention policies and schedule quarterly meetings of executives from its IT and legal operations to discuss FRCP issues, Davis said. The company also tweaked its Symantec Enterprise Vault archiving tool to make sure data is available when it's needed.

Davis recounted some questionable demands from opposing attorneys in some recent litigation in state court. One of them asked that Webcor buy his client software that could help it read the contractor's Oracle database. Fulfilling such a request could prove "very costly," said Davis, adding, "This is why [FRCP] is a new slippery slope."

Laura Dubois, an analyst at IDC, said the FRCP changes are forcing companies to significantly increase spending on backup applications. The research firm predicts that e-mail archiving application sales will grow from \$631 million in 2007 to \$1.37 billion in 2011, she noted.

The updated FRCP rules have already placed a heavy burden on IT staffers, said Howard Nirken, a partner at Austin law firm DuBois, Bryant & Campbell LLP.

"[FRCP] has made their lives incredibly complicated," Nirken said. IT is now responsible for immediately locating electronic files that "can exist just about anywhere — in networks, in people's personal computers [or] on any electronic media you can imagine."

Nirken, whose firm uses MessageOne Inc.'s hosted e-discovery system, said IT managers must make sure that such technology can freeze documents in e-mail in-boxes and instantly search for and locate needed data.

Silver Lining

The rush to comply with the updated rules has provided some businesses with unexpected benefits by forcing action, IT managers say.

Bill Shaw, MIS director of The Village of Niles, Ill., said the revised rules led city officials to decree that all e-mails to and from city offices are official documents and subject to legal review.

That policy change quickly eased the city's e-mail storage and management burden by reducing the number of nonbusiness e-mails that pass through its systems, Shaw said. "It's had a reduction in our e-mail and an increase in productivity," he noted.

The Village of Niles uses a messaging appliance called Plug n Comply from Jatheon Technologies Inc., and Shaw checks it monthly to identify non-work-related messages and other inappropriate e-mail.

The city decided to deploy Toronto-based Jatheon's appliance in early 2007 after state officials began requiring that all e-mail communication be available when needed as evidence in court cases.

The city, which employs some 250 full-time workers and about 5,500 part-timers, processes e-mail through a single Microsoft Exchange server, Shaw said.

The Brink's Co., a Richmond, Va.-based firm whose holdings include Brink's Inc. and Brink's Home Security, hopes the revised FRCP guidelines clarify which data needs to be retained for long periods and which data can be deleted, said Suzanne Barasch, manager of corporate information systems and global messaging.

The company currently purchases 20 800GB backup tapes monthly to save all of its corporate data, she said.

"I'm not able to overwrite any of my tapes, and I haven't been able to do that for three years. [Our lawyers] don't want to overwrite any data," Barasch said. "I think there comes a point where keeping everything is silly. There are files that haven't been touched in years."

Brink's will begin installing IBM's DB2 CommonStore for Lotus Domino and eMail Search for CommonStore this month to smooth what can be a crippling archiving process, Barasch said. "If someone were to come to me and say, 'Provide this [electronic evidence],' it would cause me a lot of heartache now because of how things have been stored," she noted.

Rick Chin, senior vice president of IT at Pinnacle Financial Corp. in Orlando, said his company got a head start on changing its e-discovery processes after learning about looming FRCP changes at an industry conference months before the rules took effect.

The revised rules prompted Pinnacle to buy Mimosa Systems Inc.'s NearPoint e-discovery and mail archiving software in 2006 for use with its two Microsoft Exchange servers.

Chin considers himself fortunate to have learned about the revised rules long before they needed to be implemented.

"A lot of stuff that happened last Dec. 1 caught a lot of people off guard and [led] to scrambling and [confusion over] what to do," he said. "From [listening to] my peers, it's been a drain on them to add enough storage to do e-mail archiving or modify their processes."

California Expands Breach Notification Law

(January 3 & 7, 2008)

California's data breach notification law, SB 1386, has been expanded to include incidents involving unencrypted electronic medical and health insurance data. Previously, the law applied only to financial data. The law requires that a name be associated with the data to necessitate breach notification, but Social Security numbers (SSNs) do not have to be present. The law affects all state agencies and companies that do business in the state of California. The change to the law was prompted in part by a report from the World Privacy Forum that said a quarter of a million people become victims of medical identity theft every year. In addition, the law now requires that organizations holding personal health information do not disclose that information without the patient's consent.

U.S. government needs new cybersecurity steps, Symantec warns

The warning echoes similar concerns by the GAO

Grant Gross

January 07, 2008 (IDG News Service) -- U.S. government agencies need to take additional steps to protect against cybersecurity problems after a series of congressional hearings and reports exposed several weaknesses in 2007, representatives of [Symantec Corp.](#) said.

The government sector, including state and local governments, accounted for 26% of data breaches that could lead to identity theft in the first half of 2007, according to Symantec's latest Government Internet Security Threat Report, published in September. The [U.S. Government Accountability Office](#) (GAO) also issued about a dozen reports in the last six months criticizing federal agencies for not fully implementing the GAO's cybersecurity recommendations, noted Jim Russell, Symantec's vice president for the public sector.

In addition, the House of Representatives' Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity and Science and Technology hosted a series of hearings in 2007 focused on cybersecurity lapses at several government agencies, including the [Department of Homeland Security](#) and the State Department.

"You look at that, and you say, 'Why does that happen?'" Russell said.

While U.S. agencies have a set of cybersecurity rules set out in the Federal Information Security Management Act, agencies aren't held accountable when they have breaches, Russell said. Agencies don't lose funding from Congress after cybersecurity incidents, he said.

The rules don't have "a whole lot of teeth," he added.

The good news is that agencies can take more steps to fix problems, Russell said. The first step is to inventory IT assets, a job several agencies haven't accomplished. That's not always easy, Russell said.

"Let's say I'm an agency CIO," he added. "My challenge is that my environment is so dynamic with the home workforce and telecommuting. I can see why it's a challenge to see what all the assets out there are."

Russell also called on agencies to develop comprehensive cybersecurity plans, do systematic vulnerability testing, have a data backup plan and back up frequently.

Symantec expects that cybersecurity issues will come before Congress in 2008, particularly federal agency cybersecurity practices, said Kevin Richards, Symantec's federal government relations manager. This could be "the year for information security for our federal agencies," he said.

In December, Rep. William Lacy Clay, a (D-Mo.), introduced the Federal Agency Data Protection Act, which would require U.S. agencies to implement wireless data security measures. The bill would also require each agency to draft a plan to

protect itself against the dangers of peer-to-peer file-trading networks. And it would give the director of the [White House Office of Management and Budget](#) new authority to establish information security policies.

Clay's bill would write into law many OMB recommendations, Richards said. "I always make the point that these are recommendations, and it's important to codify them," he said. "It seems like our federal government IT security strategy is very reactionary and not proactive."

That bill comes in addition to Federal Agency Data Breach Protection Act, which would require federal agencies to notify constituents whose data is lost or stolen. That bill, introduced last May, is sponsored by [Rep. Tom Davis, \(R-Va.\)](#), and Sen. Norm Coleman, (R-Minn.).

Bills that would require private companies to notify customers when their personal information is stolen or lost seem to have stalled in Congress. But there still seems to be interest from lawmakers in agency cybersecurity and breach notification, Richards said. The hearings and information requests from Davis and other lawmakers are bringing to light multiple attacks and breaches at agencies, he said.

"There's no real mechanism requiring agencies to report breaches," Richards added. "Now, [lawmakers] are dedicating more resources and giving better direction."

Nearly every Window PC likely harbors an unpatched app, Secunia says

More than 95% of PCs scanned by a security tool have one or more vulnerable programs

Gregg Keizer

January 09, 2008 ([Computerworld](#)) -- Nearly all Windows computers are likely running at least one unpatched application and about four out of every ten contain 11 or more vulnerable-to-attack programs, a vulnerability tracking company said today.

According to [Secunia ASP](#), more than 95% of the PCs that have downloaded and installed its Personal Software Inspector (PSI) utility in the last week sport one or more applications for which security fixes are available.

Secunia tracked the first PSI scan after its installation to get an idea of patch status before users start to update their machines, which can also be done through the utility.

In the last seven days, said Secunia, users have installed PSI on 20,009 machines; 95.46% of them have an unpatched application on their hard drive. "There is a newer version available from the vendor that corrects one or more vulnerabilities," said Jakob Balle, Secunia's development manager, in a post to the [company's blog](#) today. "But the users have yet to install the secure version."

Some of the other statistics cited by Balle were just as damning: 41.94% of the machines scanned by PSI in the past week have 11 or more vulnerable applications; and more than two-thirds, or 67.63%, of the PCs have 6 or more unpatched programs.

"Close to all computers are running with several insecure applications installed," Balle pointed out.

And the picture is probably even darker than the one he painted. "These results should be considered 'best case' scenarios; The real numbers are likely to be worse," he said, citing the self-selected group that the data represents. "The users of the Secunia PSI are most likely more vigilant and security minded/conscious than your 'average' user."

Secunia released the free patch detection utility a year ago, but shifted it to Release Candidate 1 (RC1) stage earlier this month. The Copenhagen-based company claims nearly 191,000 users have downloaded and run the program.

PSI runs on [Windows 2000](#), XP, Vista, and Server 2003, and can be [downloaded from the Secunia site](#).

"Individual Privacy Under Threat in Europe and U.S., Report Says" Associated Press (12/30/07)

International rights group Privacy International warns that individual privacy is under threat in the United States and Europe as governments introduce surveillance and information-gathering legislation in the name of security and controlling borders. Privacy International reports that Greece, Romania, and Canada have the best privacy records of 47 countries studied, while Malaysia, Russia, and China rank the worst. Britain and the United States are ranked as "endemic surveillance societies," the

lowest-performing group. "The general trend is that privacy is being extinguished in country after country," says Privacy International director Simon Davies. "Even those countries where we expected ongoing strong privacy protection, like Germany and Canada, are sinking into the mire." In the United States, civil liberties groups have criticized the Bush administration for its involvement in domestic wiretapping, which allows monitoring of international phone calls and email messages involving people suspected of terrorist links, without a warrant. Britain was criticized for plans for a national identity card, a lack of government accountability, and the world's largest network of surveillance cameras. Davies says the loss of computer disks with personal and bank information on 25 million people in Britain highlights the risk of centralizing information on huge government databases. The report says that privacy protection is generally worsening across Western Europe while it is improving in former Communist states in Eastern Europe. The report also says concern over terrorism, immigration, and border security is driving the spread of identity and fingerprinting systems, often without regard to individual privacy, and that the trends are being fueled by the development of a "profitable surveillance industry dominated by global IT companies and the creation of numerous international treaties that frequently operate outside judicial or democratic processes."

"Q&A: New Technologies Pose Online Privacy Uncertainties, Rotenberg Claims"

Computerworld (01/02/08) ; Thibodeau, Patrick

In terms of the new perspective on privacy held by Facebook-using young people, Electronic Privacy Information Center executive director Marc Rotenberg feels the true privacy issue is that social networking sites covertly gather information to utilize for marketing purposes. In general, Rotenberg asks the question "Are companies being fair with what they do with the data they collect?" to determine whether rules need to be established to protect customer privacy. Privacy law advocates are often simply calling on companies to provide more disclosure about their practices of data collection and use. In terms of RFID tags, Rotenberg explains that many individuals in the privacy and security communities are unhappy about the Department of Homeland Security's new "vicinity read" RFID tag standard. Such tags remove the individual's ability to identify when the tag's data is being read, which breaches the principle of basic access control, says Rotenberg. Remote RFID tags could be exploited in many ways; credit card numbers that have not been encrypted, medical data, and information on overseas U.S. travelers could all be pulled by hackers, according to Rotenberg, which is why the e-Passport proposal from the U.S. State Department had to be overhauled. Rotenberg adds that EPIC has been critical of many new proposals from DHS regarding personal identification, border control, and video surveillance. Rotenberg claims many of these proposals, such as the Real ID card, have not been fully thought through, and contain many fundamental security problems. Overall, secure systems of information are those which are only utilized for their premeditated purposes.

"Breaches Plague Government Agencies"

Dark Reading (01/02/08) ; Wilson, Tim

Several cases of security breaches have highlighted government's failure to protect individuals' privacy. In Tennessee, two stolen laptops from the Davidson County Election Office contained unencrypted information, including the Social Security numbers of over 300,000 voters. A separate incident in Washington, D.C., involved a missing laptop containing Social Security numbers, birth dates, and other personal information of over 10,000 former and current members of the U.S. Air Force. In Minnesota, the Department of Commerce reported a laptop that was stolen containing personal information. A recent Washington Post article states that criminals can obtain personal information by merely browsing public records posted on the Web. The United Kingdom has also endured several security breaches involving government agencies, receiving an equal amount of backlash for failing to secure the public's personal information.

"GAO: IRS Has Fixed Only 30 Percent of Security Gaps"

Federal Computer Week (01/08/08) ; Mosquera, Mary

A recent review conducted by the Government Accountability Office uncovered 98 weaknesses in the IRS' information security controls. Since that review was conducted, the IRS has fixed 29 of those weaknesses. For example, the agency put in place controls for user IDs for certain critical servers, improved physical protection for its procurement system, and developed security for a key financial system. However, the remaining 69 weaknesses have yet to be resolved, according to a GAO report issued Jan. 8. The report noted that the IRS still uses passwords that are not complex, grants access to individuals who do not need it, and installs patches in an untimely manner. In its report, the GAO noted that the IRS has been slow to fix these weaknesses because it has not fully implemented an agency-wide information security program to make sure that controls are effectively established and maintained. The GAO has also called on the IRS to update its policies for configuring mainframes so they can control and log changes, identify those with security responsibilities to receive special training, and expand its scope for testing and evaluating controls.

