

BY RUSS BANHAM

Don't Become

Is your agency
management system
falling prey to the
latest group of
hackers?

Phish Food

Brian Bartosh is an agency principal who figured he knew quite a bit about technology, having immersed himself in the purchase of his agency's management system and myriad applications over the years. Then, in 2003, his agency, Top o' Michigan Insurance, was turned upside down by hackers.

Always prudent and planning ahead, Bartosh wanted a more refined system, so he switched his Internet service from AT& T to a cable company, which charged him extra for a Cisco Router that it would set up and manage. Although he was informed

“In the industry we’re considered to have a high level of automation expertise, and yet we were hacked,” he says. “That’s why I wanted to chair the committee; if it could happen to us, it could happen to others, too.”

business language to take the mystery out of security.”

Yates assembled a crackerjack team to analyze agency security issues, including Tim Woodcock, president of Courtesy Computers, Inc., a Davie, Fla.-based information technology adviser to agents. Woodcock has been working in the technology field since 1973 and was the service engineer at agency management system vendor AMS through much of the 1980s before starting his own firm. Lately, aside from consulting on IT integration issues for agents, Woodcock has built a sizable business conducting network and security audits of agency systems. From what he’s learned, many agencies are “more vulnerable than they’ve ever been” to a security breach, he says. “The sophistication of hackers, spyware and phishing expeditions has grown in the last year, undermining the best security practices and requiring constant vigilance by agency principals,” Woodcock

Make a Virus Action Plan

Implement anti-virus software, including a firewall, at the desktop, laptop, server and gateway levels to limit the threat of any virus infecting the organization. This software also can be loaded on machines not owned by the agency that employees use to access the network when out of the office. When this course is followed, be sure to adhere to any licensing and fee requirements. Many businesses scheduled daily and/or weekly scan engine and virus definition updates, as well as regular scans of mail server mailboxes. Check employees’ machines to make sure they remain current with virus protection.

Policies and procedures for handling virus outbreaks are best defined in advance of a virus infection. Possible ‘virus found’ steps include:

- Verify definitions are up to date.
- Disconnect network connection.
- Delete any infected files that were “left alone.”
- Empty quarantine.
- Empty “temporary Internet files” directory.
- Empty recycle bin.
- Run full system scan. If nothing is found, reconnect cable and resume normal business. If and infection is found, delete it and rescan.
-

-Excerpted from ACT’s “The Independent Agent’s Guide to Systems Security: What Every Agency Principal Needs to Know.”

that the high-end router had a firewall, he was not told, he says, that the firewall ports would be left open until he requested that they be closed. He blamed himself, however, for not asking question. The consequence: “Someone used us as a parasite to store an illegal movie on our server for others to download and view,” he sighs.

The movie – “The Incredible Hulk”- created a storm of activity as thousands of illegal users “pirated” the film from Top o’ Michigan. “Our system performance suffered because of all the hits we received by users pulling the movie off,” Bartosh explains. He quickly installed a set of new firewalls from SonicWALL and the illegitimate traffic came to a halt. While Internet users still try to access the movie, they have dwindled in number as they realize the ports are now closed.

Bartosh learned a lesson that he is passing on to other agents in the new Agents Council for Technology paper “The Independent Agent’s Guide to Systems Security: What Every Agency Principal Needs to Know.” He chaired the task force of agents, carrier executives, technology consultants and agency software principals that produced the dense (37-page), comprehensive and absolute-must-read report. After his experience, who could blame him?

Re-ACT Now

Are other agents similarly at risk? According to a survey released in April by IVANS Inc., Internet security is a major concern for independent agents, with 80% most worried about viruses and worms. Hackers also are an issue, with 42% of survey respondents citing them as the second-biggest worry. “Smaller businesses, like independent agencies, can be more vulnerable because they often have smaller IT staffs,” states Clare DeNicola, president and CEO of the networking and ecommerce solutions provider.

Jeffrey Yates, ACT’s impassioned executive director since its founding, says the subject of security is an intimidating on for agents-hence, the new ACT report. “The risks of viruses, intrusions, identity theft, phishing, spyware and other threats to agency and customer data are real and growing,” Yates says. “This is really a never-ending issue, and we wanted to raise the awareness on the part of agency principals to the various threats and the guidance they can take to protect themselves and their customers.” He adds that the guide “is customized to the needs of agents and written in non-technical

explains.



Hackers Get Sophisticated

Phishing is a form of social engineering (read: con artistry) whereby a hacker sends a formal-looking e-mail to a system user under the guise of an ISP like AmericaOnline, a bank like U.S. Bank, an insurance carrier or even the agency's own security department, requesting information such as the user's password and login name. Often, the e-mail looks perfectly legitimate, luring unsuspecting CSRs and other agency staff into the trap. "It's gotten to the point where even I am mesmerized by phishing expeditions," Woodcock says. "The sophistication of their social engineering skills boggles the mind." Today's hackers no longer are in the game purely for kudos from their fellow miscreants. Money is the motive, particularly when it comes to stealing someone's identity to make illegal purchases. Take the case of the hackers who recently penetrated the database of ChoicePoint Inc., which maintains one of the largest databases of personal information in the country. The hackers ultimately stole the financial information of an alleged 400,000 consumers, law authorities contend. ChoicePoint's database of 10 billion business and personal records contains information such as names, addresses, Social Security numbers and credit reports.

"They were totally compromised, and thanks to a law in California, they could not keep the vulnerability hidden, as many companies like to do," Woodcock says. "In this day and age, few people haven't had to void a credit card because someone other than them has made an illegal purchase using it."

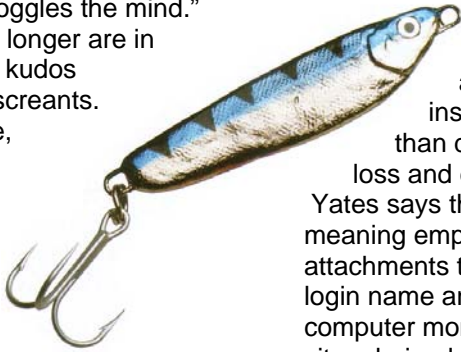
Audits Reveal Security Flaws

Woodcock's security audits of agencies usually yield a security problem. He recently audited the technology of an agency whose system was inexplicably lethargic. "They thought they had a firewall; they didn't," he says. "They thought they had intrusion protection; they didn't. Their antivirus software was archaic and they had not updated the system for new viral patterns. They had also

failed to renew their subscription to the service providing tape back up of their data and for a full year went without backup. There was no anti-spam or anti-spyware protection on the system and as far as passwords, they were non-existent. Anyone could log on as an administrator and would have full rights and capabilities. If we could put a name on this agency it would be: 'Lucky.'

Sharpening his microscope, Woodcock discovered a Petri dish of viruses, Trojans, worms, spam and other insidious "creatures." It was amazing they were still operating," he says.

Not all agencies are as lax about their security, of course. But, given the vast amounts of information traveling between customer, agency and carrier-insurance is nothing more than data, after all- the risk of loss and damage is unquestioned. Yates says the usual culprits are well-meaning employees who open e-mail attachments they shouldn't, post their login name and password on their computer monitors or access Web sites during lunch hours that are non-business-related. New risks are emerging, too, such as



Instant Messaging Woes

More and more agencies are starting to use instant messaging as well as e-mail to conduct business. Instant messaging can expose agency systems to viruses and worms in an even more insidious way than e-mail because the virus or worm can be spread through a weakness in the instant messaging software without the need for a user to open an attachment. Agencies that use instant messaging should seek virus and worm protection software that also protects instant messaging applications.

Also, some people "troll" IM users and try to get them to respond, often for illegitimate reasons.

Instant messaging can create other exposures for a business. IM "style" is typically a very loose, free-form style, and may be overly casual, or use language or expressions not appropriate for use in customer interactions.

-Excerpted from ACT's "The Independent Agent's Guide to Systems Security: What Every Agency Principal Needs to Know."

those arising from wireless technology.

"I know of an agent whose Internet service went down and he used his neighbor's wireless hub to get out," Bartosh says. "There are so many wireless hubs left open all over the place. Many agencies are buying these wireless laptops or systems out of the box and are exposing their entire network to some guy in the parking lot. And they just don't know it."

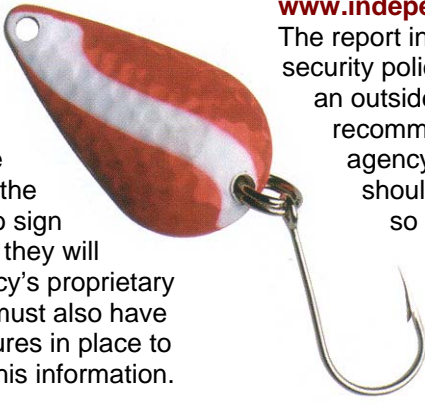
Analyze Your Risks

The ACT report cites all the dire threats to agencies, defining them for the least technologically minded person to understand thoroughly. The report also offers a self-assessment tool for agents, a very detailed outline of risks in which the agency assesses its security against different threats, from viruses to the newest security issues. "I just read about Pharming, in which hackers redirect users from legitimate commercial Web sites they wanted to visit to malicious ones that they control," Yates notes. "The fake sites look pretty much like the real thing. However, when unsuspecting users enter in their login name and password, the information is captured by criminals."

Doug Johnston, executive vice president of agency management system vendor Applied Systems, Inc., was another member of the ACT squad studying security in preparation for the report. Aside from the 'people risks' that can cause security breaches, Johnston cites the exposure to data loss or damage that the exchange of information between agencies and insurers causes. "Agents need to ask themselves when they submit an application from their agencies to an insurance company, 'How is this occurring?'" he says. "Is it through IVANS or is it over the public Internet? Is the data encrypted? Is the agency utilizing a screen scraping service where a system takes the data from your system and acts as a data entry person behind the scenes? When you're keying in personal lines data on a customer with a \$3 million house and a \$4 million personal articles schedule and then sending it over the public Internet where anybody can snoop, you have to ask these kinds of questions. In know the larger agencies and the bank-owned agencies are beginning to do this, but more mainstream agencies must do it as well."

Johnston also has caveats about agencies encountering what he

calls the "ChoicePoint debacle." As he sees it, agencies are responsible for the data they obtain from organizations like ChoicePoint, state motor vehicle departments, credit agencies and other sources. "There are people practices to be considered, including the need for employees to sign a contract stating that they will not disclose the agency's proprietary data," he says. "You must also have proper security measures in place to safeguard and store this information.



As Congress takes a look at the ChoicePoint incident, agents will need to examine their workflow processes to ensure certain people are not privy to the chain of information. They are potentially liable for this information if it gets in the wrong hands, which is hard for them since they've been told they're the ones that must order the information in the first place. They're accepting an exposure they maybe don't want."

Woodcock cites another agency security risk-complacency. "I've consulted to agencies where it's like the old saying-'You can lead a horse to water but you cannot make it drink,'" he says. "I remember this one near-and-dear client that had 45 users on a system at a single location. They had no control over their existing network. And they were loath to reinvest in technology to increase performance, save downtime and secure data. I talked to them 'til I was blue in the face, but they were the perfect example of an S corporation, taking profits out of the agency and putting the bare minimum into keeping the system up and running. Eventually, it all fell apart: The backup failed and they lost two months of e-mail data. The tape was backing up nothing."

Get Going

So what's the first thing an agency must do to keep hackers at bay? "Understand, acknowledge and communicate the importance of security," Yates says. Agency principals need to determine "where the agency currently stands with regard to security, and then take appropriate action." He advises taking ACT's self-assessment test or hiring a consultant to put the agency through a rigorous security audit.

The most important security agenda for agents is to download the ACT report immediately (found at www.independentagent.com/act). The report includes a sample agency security policy, guidance on choosing an outside security consultant and recommendations to assist an agency to prepare in advance should a security breach occur, so that the agency does not have to resort to ad hoc action after the fact.

The latter has special meaning for Bartosh, whose own quick reaction to his agency's security breach kept downtime to a minimum. "ACT believes it is vital for the agency principal to understand the security risks that his or her agency faces, to communicate the importance of security throughout the agency and then to oversee the agency's efforts to develop and then implement a comprehensive security policy," he says.

Having battled and beat the Incredible Hulk, his comments bear scrutiny.

Banham (bwriter@aol.com) is an IA senior contributing writer.

This article can be found in the June 2005 issue of the Independent Agent Magazine.



**ASSISTING AGENTS
AND BROKERS WITH
THEIR IT NEEDS
SINCE 1986**

- INFORMATION TECHNOLOGY CONSULTANTS
- NETWORK SECURITY ASSESSMENT & REPORTING
- NETWORK INTEGRATION & MANAGED SERVICES
- SAFE, SECURE, EASY-TO-USE ONLINE DATA BACKUP SERVICES
- HELP DESK SPECIALISTS

954-321-8605
www.courtesycomputers.com
info@courtesycomputers.com

 **COURTESY
COMPUTERS** INC.
WE MAKE IT SIMPLE