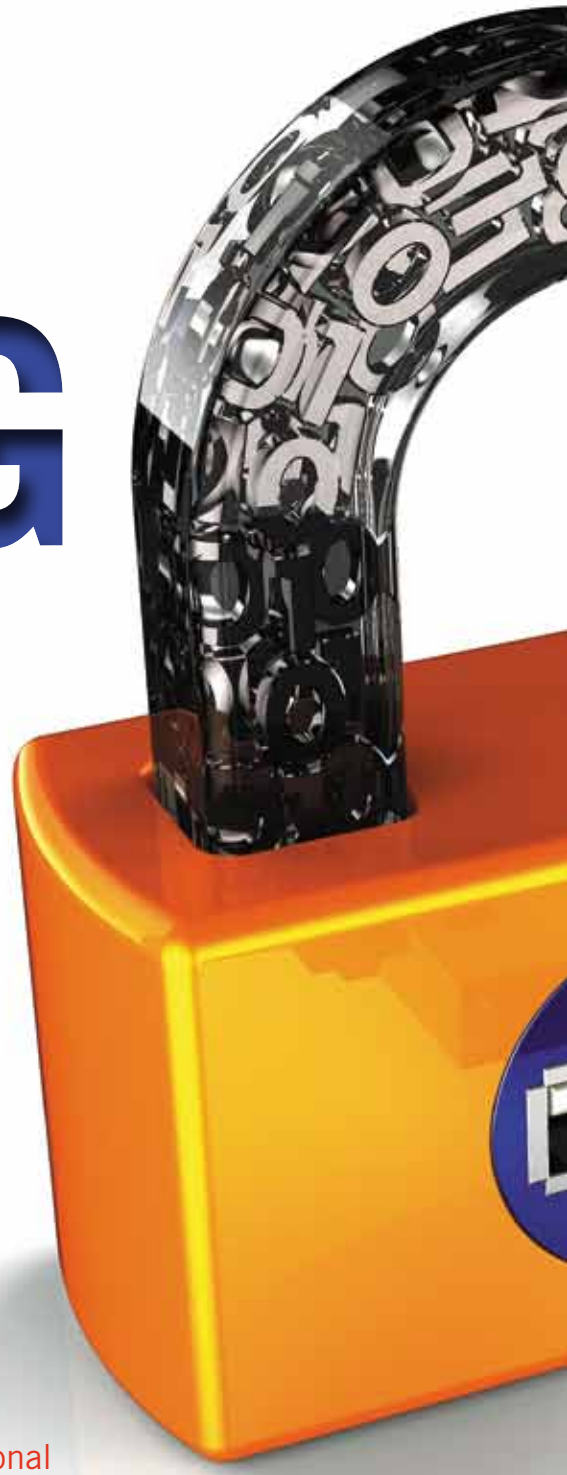
BY RUSS BANHAM

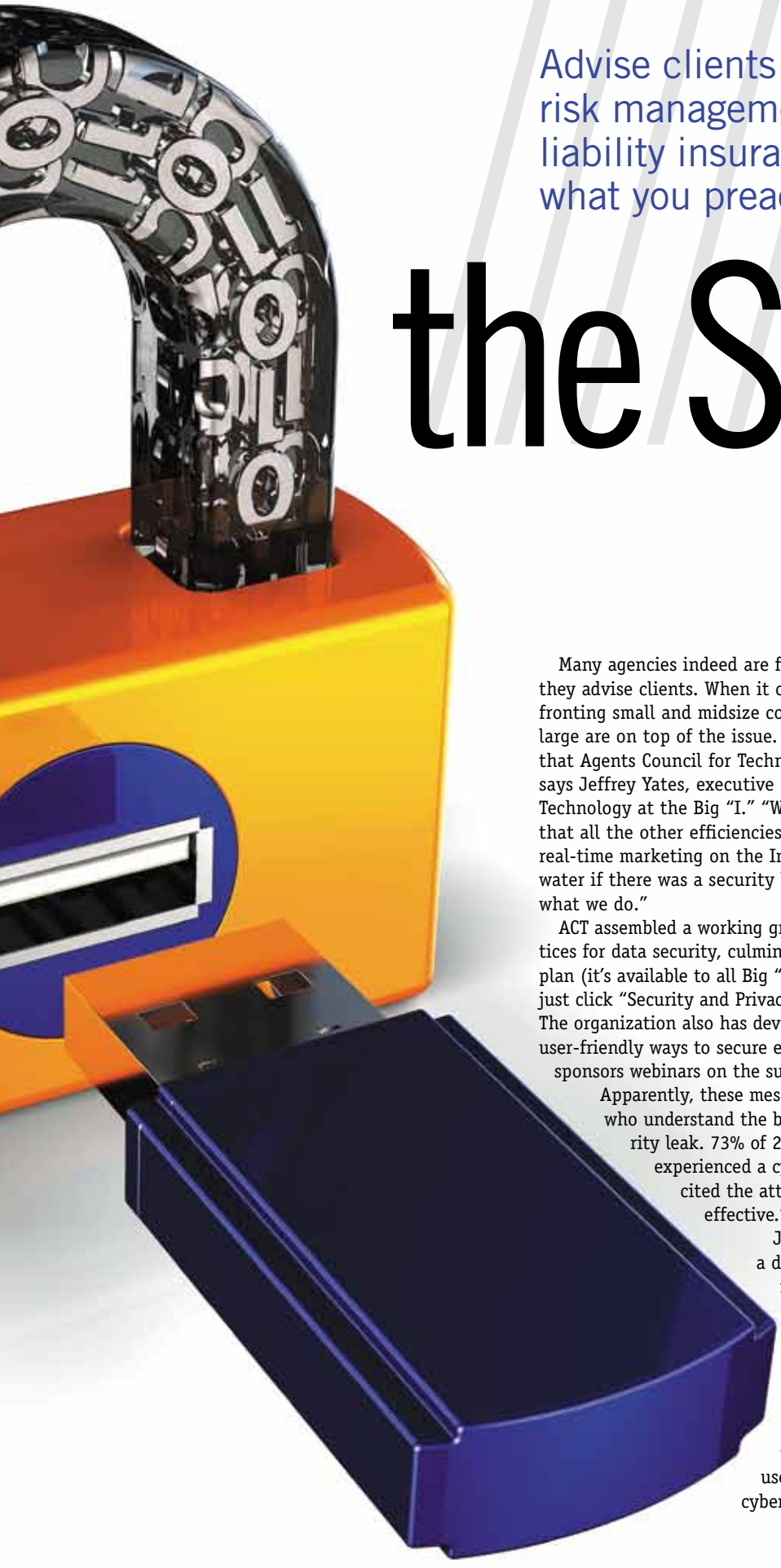
LOCKING UP



The theft or loss of employee and customer personally identifiable information is a rising liability for small and medium size enterprises. Hackers are increasingly targeting SMEs, knowing these businesses have a storehouse of personal information but are less likely than larger organizations to secure it.

But what about a very specific type of SME—independent insurance agencies? Few organizations possess the breadth of customer information in their databases and through their routine correspondence with carriers than an insurance agency. While agents advise clients on data breach risk management protocols and the purchase of first-party and third-party cyber liability insurance, the question is—are they drinking their own Kool-Aid?

SNAKE3D/VEER



Advise clients on data breach risk management and cyber liability insurance—and practice what you preach.

the Shop

Many agencies indeed are following the same prudent steps they advise clients. When it comes to the cyber liabilities confronting small and midsize concerns, insurance agencies by and large are on top of the issue. "This is one of the major programs that Agents Council for Technology (ACT) gets involved in," says Jeffrey Yates, executive director of the Agents Council for Technology at the Big "I." "We understood from the beginning that all the other efficiencies that agencies strive for, such as real-time marketing on the Internet, would be blown out of the water if there was a security breach. This is an essential part of what we do."

ACT assembled a working group of agents to develop best practices for data security, culminating in a prototype agency security plan (it's available to all Big "I" members at **www.iiaba.net/act**—just click "Security and Privacy" on the left side of the page). The organization also has developed with carriers and vendors user-friendly ways to secure email and websites, and it regularly sponsors webinars on the subject of agency security.

Apparently, these messages are getting through agents who understand the business hazards posed by a security leak. 73% of 2,100 SMEs in a survey by Symantec experienced a cyber attack in 2010. Of these, 30% cited the attacks as "somewhat or extremely effective."

Just how vulnerable are agencies to a data breach? Of 761 data breaches investigated by the U.S. Secret Service and Verizon Communications Inc.'s forensics analysis unit in 2010, 482 of them (63%) occurred at companies with 100 or fewer employees, a metric that describes many agencies. Don't expect hackers to give up either. "As more agencies use mobile devices," Yates says, "their cyber risks are proliferating."

Rules and Regulations

Approximately 46 states currently have laws on the books regarding the notification of individuals whose personally identifiable information has been stolen or lost. Aside from these state data breach laws, agencies also are subject to federal laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act, each requiring that specific actions be taken to protect consumers' non-public personal information.

Massachusetts has passed the nation's stiffest data security law; it applies to any entity interacting with residents in situations where the exchange of personal data may have occurred; as the law states, "all persons that own, license, store or maintain personal information about a resident" of Massachusetts are subject to the regulation. Thus, an agent in California who sells an insurance policy online to someone in Massachusetts, and in the course of this transaction receives and stores the person's identifiable information, is in for a harsh surprise if this data is stolen or lost.

How harsh? The regulation (201 CMR 17.00) requires the business, well in advance of a potential data breach, to assemble a written plan explaining the steps it is taking to protect personally identifiable information it stores electronically or on paper. This plan must be routinely audited. The law further requires that email containing "personal information" be sent in an encrypted manner. This would include, for example, personal information submitted by an agent on a commercial lines application. Moreover, the law requires that personal information contained on laptops and mobile devices be encrypted because of the higher risk that these devices will be lost or stolen.

Now, if personal data is indeed lost, leaked or stolen, potentially serious consequences await. Massachusetts General Law, Chapter 93A, Section 4, authorizes the attorney general to seek injunctive relief, which may involve a court-imposed $5,000 civil penalty per violation. That's just one person's personally identifiable information; the potentially crushing damages in a breach involving hundreds of affected people give serious pause for consideration.

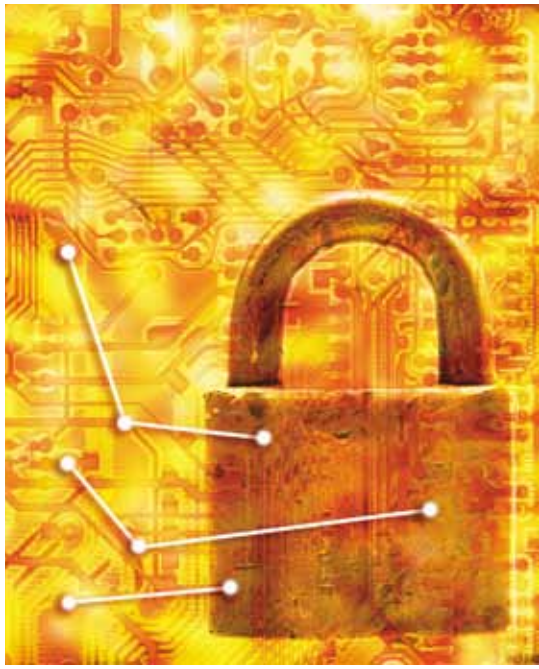
Then, there are the legal defense costs if an action is brought against the entity, not to mention the dire risk of reputational harm if the public becomes aware of the incident. Even a business not specifically subject to 201 CMR 17.00 may incur significant defense and settlement costs, if, for instance, the plaintiff attorney contends that Massachusetts' personal information security law is effectively the standard of care for safeguarding private data.

Other possible costs include the need to notify affected parties of the breach and provide credit-monitoring services to assess if the individuals' bank accounts and credit cards have been violated. In cases of a comprehensive breach, the business may need to hire a network security expert to determine the technological causes of the breach, and a crisis management firm to handle the public relations fallout.

Steven J. Aronson, president of Aronson Insurance, is especially cognizant of the Massachusetts law, given the agency's two locations in Needham and Newton in the state. Aronson recently was asked by the Big "I" and the Massachusetts Association of Insurance Agents to assess the law's impact on the agency system, in order to train agents to ensure effective compliance. "There is no need for an agency to research each state's data privacy laws, since if you just follow the law here you will be in pretty good shape," Aronson says. "It's the most onerous one out there."

In his own agency, Aronson has made great strides securing his customers' and employees' personally identifiable information. "Most people forget that technology is not the only way for a criminal to get at this stuff," he says. "The first thing I advise is to lock the windows and doors, and install a central station burglar alarm. You'd be amazed at how easy it is to steal a server or a drawer's worth of files."

He adds, "Of course, this is just the first step."



GARY S CHAPMAN/GETTY IMAGES

Serious Stuff

Many agents like Stan Burnett take the threat of a data breach seriously. "We were an early adopter of technology, purchasing an imaging system that was connected to our servers about 14 years ago," says Burnette, president of Burnette Insurance Services in Suwanee, Ga. "Within a week, the firewall was hit with thousands of hackings. We were scared to death. Then, someone hacked into the computers and destroyed our database—didn't steal the data, just blew it up. That's when we realized we needed help."

The agency brought in MIS Solutions, a managed services provider also based in Suwanee. MIS beefed up the firewalls, layered in a range of different passwords for employees to ensure they perused only those files specifically related to their work, and policed the flow of information from customers though the agency to carriers. For instance, when the agency receives a client's payroll census for workers compensation, the employees' personally identifiable information is deleted so all that remains is the actual dollar figures of the claim.

More recently, the agency implemented a decoder in mobile devices like smartphones and laptops that secures remote

Simple Security

When it comes to avoiding a data breach at your agency, heed these pieces of advice:

- Make sure that passwords for desktop PCs have eight characters, a mix of upper case letters, lower case letters and numerals.
- Do not put any customer data on a laptop, smartphone or thumb drive unless it is password protected.
- Use an email encryption service like AppRiver or RPost for emails that contain information that would be embarrassing if intercepted.
- Upgrade hardware and download the latest versions of software to ensure the latest security protections, and keep the agency current on both hardware and software versions in the future.
- Make sure that third-party vendors that possess your agency's private information have equivalent security plans and procedures in place.
- Thoroughly inform and train all employees on the agency's new security plan, procedures and workflows, and monitor their adherence to these plans and procedures.
- Monitor all traffic moving through systems for any unusual activity and consider periodic security audits by external security professionals.

—R.B.

communications outside the agency's firewalls. "The device changes the code every 30 seconds," Burnette notes. "Users carry a little fob to get the code of the minute; otherwise they can't log on."

Despite these best practices, Liam Holmes, CEO of MIS Solutions, says hackers remain undeterred in their quests. "I just ran a report last month and there were 32,000 unauthorized attempts to penetrate the firewall (at Burnette)," he explains. "None of them got through."

Some agencies have determined the risk of a data breach requires internal assistance from IT specialists (ACT advises that all agencies consider the appointment of a data security coordinator to develop and implement the agency's security program). At Eustis Insurance & Benefits, Keith Oufnac is that person. "Our biggest problem is security," says Oufnac, vice president of information technology at the New Orleans-based agency.

Among the best practices Oufnac has implemented is secure email. All email is downloaded and filtered by Postini, an email security and archiving service now owned by Google. The Postini Communications Suite eliminates unwanted content from email, instant messaging and the Web, and it automatically encrypts sensitive messages between business partners, such as an agency and a carrier. "We do this to protect everyone, since everyone is vulnerable to social engineering scams," says Eufnac.

Social engineering—or phishing, as it is sometimes called—is getting more sophisticated. Most everyone by now has been a target of an official looking email that purports to come from a bank or some other service provider. The email strongly recommends that you download an attached link. If you make the mistake of doing this, the link will imbed a keylogger in your computer that records your keystrokes, with the goal of capturing user ID and password details. Once in the system or network, the hacker can easily find a way into a database of customer or employee personally identifiable information.

"Just last month, an employee here reported that he received an email from support@eustis.com, which looked very real," says Eufnac. "I was apprised and immediately wrote back—'delete, delete, delete.'"

To determine if a hacker is trying to penetrate the agency's firewall, Eufnac has installed intrusion detection software. "All our traffic is analyzed and updated every day, and since we have a 'hub and spoke' network with our remote offices, we encrypt all messages going back and forth," he says. "We also publish a security handbook and make each employee sign off that they have read it."

Aronson has similarly drafted an information security plan, and the agency trains employees on safe data practices. Its version is based on the aforementioned plan on ACT's website. The agency uses TLS (Transport Layer Security)—cryptographic protocols that ensure secure communications over the Internet—which all agents should consider implementing to secure interactions with insurance company partners. Finally, the agency makes sure all transfer requests between servers and browsers have a secure hypertext transfer protocol (https). "If you see https in front of the URL, this indicates that you are now in a 'secure session,'" Aronson explains.

Insurance Just In Case

Each of the agencies in this article does something else besides implement data security and risk management best practices—they buy cyber liability insurance. "In today's world, you simply must have it," says Eufnac.

"I bought the coverage last year," Burnette agrees. "Our E&O carrier offered it as an extension to the policy we had. We're selling a lot of network security and privacy coverage to our customers, and I felt we just had to have it too." Aronson notes that his E&O carrier didn't start offering the coverage until recently, but as soon as it became available he jumped on it.

ACT's Yates warns that E&O carriers aren't just giving away the coverage for the heck of it. "There is now coverage in many cases for a data breach, but it is often predicated on the agency having a written security plan, secure email and website, and other best practices in play," he explains.

Risk management first, and then insurance: good sense for all SMEs. IA

Banham (**russ@russbanham.com**) is an IA senior contributing writer.