127 S. Peyton St. Alexandria, VA
800.221.7917
www.independentagent.com/act

About this article: *This article discusses the importance of agencies' implementing a written security plan and program and the free prototype agency information security plan that ACT has developed to assist agents. The article then provides agencies with a series of steps to take to put a strong security program in place, customized to their particular operations.*

ACT Releases Prototype Agency Information Security Plan

By Jeff Yates, ACT Executive Director

Recent headlines have underscored the importance of agents having written security plans to protect the security of their operations and the privacy of their clients' personal information. Not only could a breach of clients' personal information devastate an agency's reputation; it is likely to result in the agency's having to undertake time consuming and costly actions on behalf of clients whose personal information is compromised.

We are aware of agents being fined in at least two states for not having a written security plan and of a major firm recently having to announce two data breaches, one occurring online and the other when a laptop containing confidential personal information was stolen. Just as a well managed agency takes specific steps to protect against E&O risk, it needs to have a written security plan, incorporate the plan into its procedures, train its employees to implement these procedures consistently, and monitor for compliance.

ACT's Information Security Plan

ACT has developed a free prototype security plan to assist agents and brokers in formulating and implementing specific procedures, training and monitoring to protect the security of their operations and the privacy of their client information. The plan is the product of ACT's Agency Security Best Practices Work Group, with assistance from ACT's Security Issues Work Group and IIABA's Office of General Counsel. We owe the Massachusetts Association of Insurance Agents special thanks for making the plan it had developed for its members available to us, which we used as a starting point for our plan.

Before sitting down to develop your agency's security plan, or to refine your current plan, it is essential for you to be thoroughly familiar with your state's data breach notification and privacy laws, your insurance laws and regulations, applicable federal laws and regulations, as well as the laws of any states where you hold nonresident licenses or possess personal information on the state's residents. This will enable you to conform your agency's plan to these requirements. We used the Massachusetts privacy law as a starting point for the ACT prototype plan, because Massachusetts imposes some of the most specific requirements.

Before providing some specific guidance on how best to use the ACT prototype plan in your agency, it is important to provide you with a brief overview of some of these laws and regulations.

State & Federal Privacy Laws

Agents need to be aware of the general business and insurance specific security and privacy laws, regulations and administrative letters that apply to them in their resident states, as well as in states where they hold non-resident licenses or where individuals they insure are resident. For example, the Massachusetts privacy law applies to "all persons that own, license, store or maintain personal information about a resident" of Massachusetts. Similarly, the recent August, 2010 Connecticut Insurance Bulletin applies whenever there is an "unauthorized acquisition or transfer of, or access to" the personal information of any Connecticut resident, even if the data is encrypted, and the Insurance Department must be notified within five days from when the "information security incident" is identified.

The federal Gramm-Leach-Bliley Act (GLB Act) requires businesses to proactively implement administrative, technical, and physical safeguards to protect customer non-public personal information. Many states have enacted laws and regulations to implement the GLB Act for the insurance industry in their state. Overlay onto these requirements the Security Breach Notification laws that have passed in 46 states and the District of Columbia.

We are now starting to see state privacy laws move from the implementation of general safeguards to much more specific requirements. For example, the Nevada law and Massachusetts law (March 1, 2010) specifically require that email containing "personal information" be sent in an encrypted manner. This would include, for example, personal information submitted on commercial applications. The Massachusetts law in addition would require the encryption of personal information contained on laptops and mobile devices because of the higher risk posed that these devices will be lost or stolen.

Implementing Your Agency's Security Program

After familiarizing yourself with the laws and regulations that apply to you, you are ready to develop or refine your own Information Security Plan using the ACT prototype plan as a starting point. It is important that you either use ACT's prototype plan as a checklist or customize its terms to fit your particular agency's operations. The various state and federal laws typically provide that the administrative, technical, electronic and physical safeguards a business incorporates into its security program be appropriate to the size and complexity of the business and the nature and scope of its activities.

ACT prototype plan also contains a series of "Notes" designed to help agencies in customizing the plan and pointing out the need to consult additional laws that might apply to your agency. A good example is the Note on HIPAA, pointing out that if the agency is a "Business Associate" handling "protected health information" ("PHI"), there

are additional specific security requirements that the agency would need to add to the prototype plan, along with some resources for the agency to consult.

Consider taking the following implementation steps:

1. Appoint a Data Security Coordinator who will oversee the development and implementation of your agency's security program.
2. Ascertain all of the types of private client and employee information that your agency retains, every place where it is stored (whether in paper or electronic format), exactly who has access to it and how it is used and transmitted. Be particularly sensitive to the types of private information that are singled out in the privacy and data breach laws that are applicable to you.
3. Decide whether you really need to store or transmit all of this private information that you possess, and if not, don't keep it. If you do need to possess it, restrict its access to only those employees who need to use it, keep it off PCs, mobile devices and home computers, and encrypt it wherever it is stored (where possible) and when it is transmitted.
4. Have an employee team go through the prototype plan and customize it to your agency's operations and develop new procedures and workflows as necessary to implement it.
5. Acquire or upgrade your hardware and move to the latest versions of your software so that you incorporate the latest security protections, and then keep your agency current on both hardware and software versions in the future.
6. Thoroughly train all employees on your agency's new security plan and any accompanying new procedures and workflows, and secure their written commitment that they will abide by the plan. Change your procedures so that new hires are immediately trained on the security plan. Make sure your procedures assure that the access of terminated employees is cut off immediately from the agency's systems, as well as from any carrier websites or other third party sites. *Ongoing employee training and reminders about your security requirements and protecting clients' private information are absolutely key*, because security breaches often result from employee error or a lack of sensitivity to protecting this information.
7. Make sure that third party vendors that possess any of your agency's private information have equivalent security plans and procedures in place, as well as a strong commitment to security and protecting this information.
8. Monitor your employees' adherence to your agency's security plan and procedures, monitor the traffic over your systems for any unusual activity and consider periodic security audits by an outside security professional.
9. Review and update your security plan, procedures and workflows at least annually.

The Big Picture

One year ago ACT completed its latest report on key trends and "must do" issues the industry must tackle to be properly positioned to succeed in the future. We identified

three critical "must do" issues and the first was to increase industry awareness and collaboration on security & privacy. ACT concluded that the significant progress the industry has made with Real Time and other new workflows is directly dependent on protecting the security and privacy of the client information being used. In addition, agents have unprecedented opportunities with online marketing and servicing using their websites, social media and other Internet tools, but again, protecting the security of these mechanisms and the privacy of client information on them is critical.

ACT is committed to providing independent agencies with information and tools to help them protect the security of their operations and client information. We believe ACT's new prototype information security plan will be a major resource for agents and brokers and it provides a good example of the kind of industry collaboration on security issues that needs to occur.

Editor's note:
Please visit www.iiaba.net/act at the "Security & Privacy" quick link for ACT's free Agency Information Security Plan and other security related resources, including an online version of this article with links to the various laws and regulations mentioned.

Jeff Yates is Executive Director of the Agents Council for Technology (ACT) which is part of the Independent Insurance Agents & Brokers of America. Jeff can be reached at jeff.yates@iiaba.net. ACT's website is www.iiaba.net/act. *This article reflects the views of the author and should not be construed as an official statement by ACT.*