Protecting your Association and its Intellectual Property on Line

Presentation by Richard C. Balough to the 2007 Chicago Association Law Syjmposium of the ASAE & the Center for Association Leadership
April 18, 2007

Occasionally I am asked what is my ideal client? My response is simple. I want a client who is rich, guilty and scared.

I know that none of your associations are rich. I hope after today's presentation you won't be guilty of violating anyone's privacy or breaching any fiduciary duty concerning data or violating any federal or state laws.

As to being scared, anyone who collects, holds or transmits data containing personal or confidential information always should have some apprehension that he or she is not doing enough to protect that data.

Any entity that collects private or personally identifiable information needs to protect that data from improper disclosure. As associations, you collect the names of your members, their addresses, maybe some information as to their families. Maybe you collect other personally identifiable information such as education and date of birth. You may even have social security numbers and credit card information. All of this information needs to be protected.

Everyone has some expectation of privacy. Even when an individual gives information to a third party, there is some expectation that the third party—your association for example—will treat certain information as private and confidential.

We know today that information in a digital form can be transmitted instantly via the internet to third parties either inadvertently or by an employee. Information can be downloaded onto thumb drives and be out the door in an instant. This can be done by an employee or any third party who has access to your computers.

You can be held responsible for this loss.

How do you protect yourself in today's digital world?

There are several steps.

1. Know what data you collect.
2. Know why you are collecting the data.
3. Know where the data is located.
4. Know who has access to the data.
5. Know how the data is protected.
6. Know how data is archived and/or destroyed.

Let's discuss these in detail.

First, you need to know what data you have. Sounds obvious, yes? But what information are you collecting? Do you really know? Have you done an audit?

Second, why are you collecting the data? Do you really need all of the data you are collecting?

Third, what are you telling your members when you collect the data? What representations and warranties are you making? Are you abiding by those representations? Do you know if you are doing what you said you would do with the information?

Fourth, are you sharing the information? If so, how are you sharing the information? Does the party with whom you are sharing the information treat the information with the same degree of confidentiality as you do? How do you know?

Do you loan out or sell your email lists? What about your mailing lists? If you do, are your members aware of the policy? Have they given their consent?

Do you send out a member directory to your members? What information is contained in it?

Now that you know what data you have and why you are collecting it and with whom you are sharing it, you need to do an inventory of where you are storing the data.

Take an inventory of where your data is stored. Is it stored in a server? In individual desktop computers? On laptops? If you receive information via the internet, and who doesn't these days, does the information come directly to your server? Is it on a third party server? Is the data encrypted? Are the computers password protected? Who has the passwords? Is any of the information restricted from all of your employees or can anyone have access to it? Have you explained to your employees how to treat the data? Do you have written policies? Do you enforce the policies?

In other words, the data you collect should be secured. This should be done by passwords, levels of access so that not all employees have access to all of the information. You should have a policy to change the passwords on a regular basis. Sensitive personally identifiable information should be encrypted from the time it leaves the computer of the person sending the data and while it is stored in your server.

You also need to make sure that the security programs and firewalls are up to date. If not, you can be held liable if information is stolen by someone using known vulnerabilities for the computer program. For example, Petco stated on its website that "At Petco.com, protecting your information is our number one priority and your personal information is strictly shielded from unauthorized access. Entering your credit card number via our server is completely safe. The server encrypts all of your information and

no one except you can access it." As you can guess, that's not the way it worked out. The program that Petco used was outdated and the encryption program was not up to date. A hacker got into the site accessing credit card numbers in an unencrypted clear text. The FTC said Petco's privacy policy was deceptive and violated federal law.

Not only is the data on your current computers and servers, but it probably is on paper somewhere. When you dispose of paper with the information, do you shred the paper? If you send the paper off somewhere to be shredded, do you know that it was in fact shredded? Under the law, you are required to make sure that the third party shreds it under the Federal Trade Commission's Disposal Rule.

Oh, yes. Those old computers and servers that stored the data. When you got new computers, what did you do with the old computers? Tossed them? Gave them to charity? You know that erasing the hard drive does not delete the information, so you should take the hard drives out and destroy them. What about back up tapes and disks. Are those kept under lock and key? What is your document retention program? How and when are the back ups destroyed? Are you keeping information after it is useful?

Finally does your association have a plan where there is a security breach? Your association should maintain a log of network breaches and have an intrusion detection system in place. You need to monitor incoming traffic and watch for unexpectedly large amounts of data being transmitted form you r system to an unknown user. Have a breach response plan in place.

You need to have a culture at the association that recognizes and respects privacy and data protection at all levels.

Sometimes a simple slip up can cause huge problems. For example, Eli Lilly thought it was helping its Prozac customers when it set up an on-line system to give out information on Prozac and to help its customers use prozac by sending out emails However, when Lilly decided to do away with the email program, it sent out an email notification to all the registered users. The programmer who sent out the notice put the email addresses in the to line rather than the blind cc line. The result was that all the participants emails were available to all of the participants. The Federal Trade Commission filed an action against Lilly who agreed to pay a fine, institute a training program that key executives had to attend and required Lilly to file reports for five years.

For those of you who operate in the EU and obtain data from persons in the EU, you have additional protection concerns. While we think that the US is concerned about privacy, the restrictions in the United States actually are less than in the EU. If you do collect data from persons in the EU, you should become familiar with the EU Privacy Directive and its Safe Harbor provisions.

I want to mention two other items that should be on your radar screen.

First, the Children's OnLine Privacy Protection Act. While the act exempts non-commercial websites from its coverage, you should be aware of its provisions and attempt to comply with it. The act basically prohibits the collection of data on children who visit websites designed for children or those that attract children. What is a website that attracts children? It is a factual determination based upon content, whether there is advertising on the website directed at children, the intended audience and whether the site uses animated characters. Data can only be collected if the parents give permission for its collection. For example, Fields Cookies had on its website an offer to give free cookies to children under 12. It disseminated the childrens name, home address, email address and birth date to third parties. Hershey had a website that collected children's information but had an online consent form for children under 13. However, even if the form was not filled out, the website collected the information. In both cases, the FTC said the companies violated the COPPA. Fields had to pay $100,000 and Hershey's $85,000. There is information in your packets on COPPA.

The other item that the lawyers in the audience should b e concerned about is the transmission of metadata. Every time you create a document, modify a document or review a document, metadata is created on the document. This information can include the author, the date and changes made. There are ethical concerns in sending out documents to opposing counsel that contain this metadata as well as concerns about the receiving attorney mining the metadata. To eliminate this data, you need to scrub the document before you send it out by using special scrubbing programs.

In New York, attorneys have a duty to use reasonable care when transmitting documents by email to prevent the disclosure of metadata containing client confidences or secrets.

In Florida, an attorney sending an electronic document should take care to make sure no client confidences are contained in metadata. The receiving attorney is obligation not to try to obtain metadata from any electronic document.

I hope you take the questions raised today and use them as a framework to better protect your association's and your members' confidential and personal documents.