

Security checklist helps ensure compliance



By Bart A. Lazar

Last month, I wrote about the reasons for protecting the security of marketing and employee information (See "Guard biz data with security strategies," page 6, Oct. 15). Since last month, California has passed legislation that requires any business that owns or licenses personal information about a

California resident to take reasonable security measures to protect the personal information from unauthorized access, destruction, use, modification or disclosure. In addition, any business that shares personal information about a California resident with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures to protect the personal information from unauthorized access, destruction, use, modification or disclosure. So, although security practices were not mandated by law last month—they are now.

As promised, though, I have put together a checklist of some basic security practices for your company and clients to consider that you may want to use as one of your guides to a reasonable level of compliance.

Nontechnical security best practices:

- ◆ Recognize that corporate security is a system or group of systems that are constantly changing—it is not static.
- ◆ Security involves the commitment of resources. The line of authority to protect data security must begin at upper manage-

MARKETING AND THE LAW

ment or it will not get done or be taken seriously. Put someone with authority in charge.

- ◆ Ensure that someone outside of the IT/MIS department is involved in the accountability and reporting activity process. This is sometimes referred to as redundant reporting.

- ◆ Put together an interdisciplinary group to map strategy out—and meet. Technology, legal, financial, human relations, marketing and compliance should all be represented. International operations should be included as well.

- ◆ Many breaches can be prevented or halted through awareness. Try to make your security and privacy policies clear and understandable to employees.

- ◆ Once you have clear policies and procedures, train your management and employees on your policies and procedures so that the entire organization (top down) knows that this is important and what could be lost or gained through their efforts.

- ◆ Don't be an ostrich. Monitor developments and participate in the process through trade association activities because your trade association can help you stay involved in developing self-regulatory prin-

ciples.

- ◆ Keep an up-to-date list of service providers you may need to use in investigating security breaches, contacts at law enforcement agencies whom you may need to contact if you believe your employees are subject to an identity theft incident and contacts at the credit reporting agencies for employees to call when they fear they are the victim of identity theft.

- ◆ Put security provisions into agreements with vendors.

- ◆ Whether you handle your evaluations with internal or external resources, conduct periodic updates.

What to put in your privacy and security policies:

- ◆ Identify situations in which data is collected from employees and for what purposes the information is collected, used and disclosed.

- ◆ Before preparing your policy, consider the data that is collected and whether that data must be used. For example, entire Social Security numbers need not be used for identification purposes. Combining a person's initials (or some other code) with the last four digits of the Social Security number is likely to be sufficiently unique to identify the employee but not pose a significant identity theft risk if the information is accidentally disclosed.

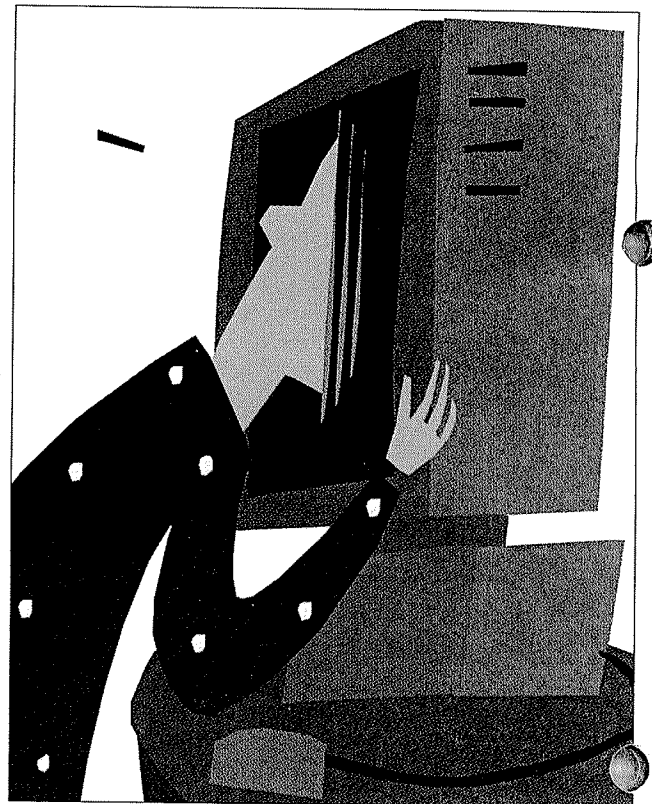
- ◆ Identify the data to be collected and how it is to be used, how long it should be retained and how it is to be disposed of.

- ◆ Identify specific categories of sensitive data (sex, race, religion, health) that may need extra protection and what extra protection or limitations on use are involved.

- ◆ Establish limitations on use of data, particularly the transmission of data in unencrypted form, when data must be encrypted and what method of encryption to use.

- ◆ Establish the employees that have access to certain categories of data.

- ◆ Establish password protocols for complexity and for changing passwords on a regular basis. (Also, passwords should not be written down on notes near computers!)



- ◆ Articulate the protocol to follow if an employee is not sure whether information can be used or disclosed in a particular manner, and if the employee becomes aware of or suspects a security breach.

- ◆ Consider establishing a separate incident response procedure establishing the method of investigating a security breach.

- ◆ Outline the potential penalties for violation of the policy.

Some basic technological and nontechnological steps to take:

- ◆ Put your compliance team together. (This is critical so it bears repeating.)

- ◆ Asset management/evaluation:
 - Inventory your record systems. This includes storage of physical (vs. electronic) files. Identity theft can still occur when an employee takes paper employment files home.

- Locate your data entry points both online and off-line—where employee data is entered, where it goes, and how it is used and retrieved.

- Collect and retain the minimum amount of personal information necessary to accomplish your business purposes.

See LAZAR / Page 10



Atlanta: Jackson Associates, Inc. 770.394.8700

Boston: Boston Field & Focus-Performance Plus 508.872.1287

Boston/Frammingham: Boston Field & Focus-Performance Plus 508.872.1287

Charlotte: Leibowitz Market Research Associates, Inc. 704.357.1961

Chicago/Downtown: National Data Research, Inc. 847.501.3200

Chicago/Northfield: National Data Research, Inc. 847.501.3200

Cincinnati: Qfact Marketing Research, Inc. 513.891.2271

Dallas: Focus on Dallas, Inc. 972.960.5850

Denver: AccuData Market Research, Inc. 800.808.3564

Detroit: MORPACE International 248.737.5300

Houston: Opinions Unlimited, Inc. 713.888.0202

Indianapolis: Herron Associates, Inc. 800.392.3828

Los Angeles/Beverly Hills: Adept Consumer Testing, Inc. 818.905.1525

Los Angeles/Encino: Adept Consumer Testing, Inc. 818.905.1525

Memphis: AccuData Market Research, Inc. 800.625.0405

Minneapolis: Focus Market Research, Inc. 612.869.8181

Northern New Jersey: Meadowlands Consumer Center, Inc. 800.998.4777

Orlando: AccuData Market Research, Inc. 800.831.7744

Philadelphia: Group Dynamics in Focus, Inc. 866.221.2038

Phoenix: Focus Market Research, Inc. 480.874.2714

Portland: Consumer Opinion Services, Inc. 503.493.2870

Providence: Performance Plus 508.872.1287

San Diego: Taylor Research, Inc. 619.299.6368

San Francisco: Nichols Research, Inc. 408.773.8200

San Francisco/Concord: Nichols Research, Inc. 408.773.8200

San Jose: Nichols Research, Inc. 408.773.8200

Seattle: Consumer Opinion Services, Inc. 206.241.6050

Tampa: The Herron Group of Tampa, Inc. 813.282.0866

Washington, D.C.: Shugart Research, Inc. 301.656.0310

ANOTHER GREAT REASON TO RETHINK
THE OLD EGG/BASKET THING

GroupNET

rewards

Now there's one more great reason to work with the largest network of independently-owned and top-rated focus group facilities. Earn just 10 Rewards certificates from any combination of GroupNet sites and receive a complimentary focus group room rental... on us. Visit group-net.com for details.

One click group-net.com | One call 800.288.8226





Why Risk Your Brand's Success? Call Brand Institute, Where Great Brands Begin!®

Brand Institute services include:

- Brand Strategy • Brand Name Development
- USAN/INN Development
- Market Research • Design

Drug Safety Institute services include:

- Regulatory Safety Name Research
- Gap Analysis • Labeling • Packaging
- Risk Management



James L. Dottoro
President and Chief Executive Officer, Brand Institute, Inc.



Jerry Phillips, R.Ph. President, Drug Safety Institute
(Former Assoc. Dir., FDA ODS/DMEIS)



BRAND INSTITUTE, Inc.
www.brandinstitute.com



Drug Safety Institute®
A Subsidiary of BRAND INSTITUTE, Inc.
www.drugsafetyinstitute.com

CHICAGO (312) 475-9600

DALLAS (214) 515-9022

MIAMI (305) 374-2500

NEW YORK (212) 557-2100

RALEIGH (919) 572-9311

ROCKVILLE (301) 984-1055

SAH DIEGO (619) 455-1000

SAH FRANCISCO (650) 961-5100

SWITZERLAND +41 (0)21 619 9000

LAZAR / From page 6*Employ tech safeguards,
closely screen personnel*

—Classify personal information in records systems according to sensitivity.

◆ Employ appropriate physical and technological safeguards.

—Restrict employee access to information necessary to perform job responsibilities.

—Use appropriate technical means to restrict access to data. Don't forget physical files and the importance of locks and security guards as well as firewalls and passwords.

—Establish a means of monitoring access to data.

—Terminate access privileges immediately for former employees and contractors.

◆ Promote security awareness.

—Develop and implement policies and procedures.

—Maintain ongoing training and communication.

—Monitor employee compliance.

—Impose penalties for noncompliance.

◆ Require third parties to comply.

—Enter into contracts with service providers and business partners.

—Monitor and enforce third-party compliance.

◆ Employ and test technology.

—Learn the capabilities of the technology you already have in place. Most companies do not use all of the technology they own or license. You may not need to acquire as much technology as you think.

—Create intrusion detection.

—Install data encryption.

◆ Evaluate your personnel.

—Screen personnel for positions with access to data.

—Include security in job responsibilities.

—Establish confidentiality agreements with employees.

◆ Develop an incident response protocol.

◆ Dispose of data appropriately.

◆ Review (and potentially test) your security plan annually. ■

Bart A. Lazar is a partner who specializes in counseling, business transactions and litigation in intellectual property, advertising and promotions, privacy, Internet and related matters for Chicago-based Seyfarth Shaw LLP. He can be reached by e-mail at BLazar@seyfarth.com or news@ama.org.

Know. Now.

*Obtain con
in less than
expert ma
you can tr*



Reach the only people who can tell you if your latest *idea* is your next best *product*.

Only InsightExpress® can deliver concept screening, testing, and attitude & opinion research you need in 24 hours from need identification to results delivery. Our unique recruitment methodology provides leading CPG firms with access to more than 100 million individuals.

InsightExpress' patented and award winning solutions empower you to make the right business decisions about your ideas in real-time. It's concept testing without breaking your budget, at a speed that won't impact your momentum.

Leading consumer package companies turn to InsightExpress' market research expertise for all of their research needs. See why by calling InsightExpress' research experts at 877-329-1552.

Visit www.insightexpress.com/concepttest to learn more about InsightExpress and for a white paper detailing how to successfully migrate traditional testing online.