

# Privacy & Security Law Update

## New Year's Resolution #1 Security Program Check-Up

Information security programs enable companies to meet their legal and business objectives by managing the multitude of risks associated with use of information and technology.

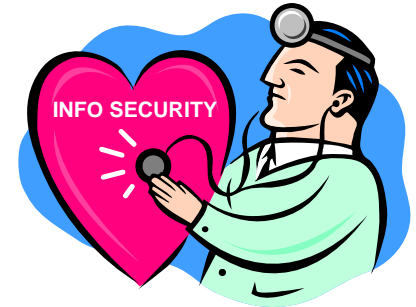
With the ever-growing scrutiny of corporate security, it is an excellent time to evaluate your company's security program and verify that it meets legal requirements and manages risk sufficiently. Effective security programs contain five key components: (1) risk assessments to identify threats and vulnerabilities; (2) strategy development to prioritize and mitigate the risks; (3) controls implementation to assign responsibilities and deploy specific processes to manage risks; (4) testing to confirm that risks are appropriately mitigated by



the controls; and (5) monitoring to adjust of the controls given emerging threats. The safeguards should reflect the sensitivity of the information being protected.

The following checklist presents basic questions that can help you evaluate your company's security program.

- Do you have a designated individual who is responsible for the security program? Are your current controls and security processes documented? Is the program approved by your Board of Directors or senior management?
- Do you classify your information assets based on the sensitivity of the data elements?
- Do you have an inventory of your information assets,



software and hardware devices? Do you have an inventory of information and technology maintained by service providers?

Have you identified and prioritized internal and external threats to your information and systems? Did you include threats from technical and organizational vulnerabilities (such as ineffective training), individuals with malicious intent, accidental loss or damage, and environ-

*continued on page 2*

### IN THE SPOTLIGHT... Russia's Privacy Law

The Russian federal law on personal data takes effect this month, establishing an EU-style privacy regime in Russia.

The law applies to all personal data, including HR data. Companies may process personal data only if required by Russian law, as needed to effect an agreement between the parties, to protect a "vital interest" of the data subject, or with the data subject's consent. Written consent is required to process sensitive information, including biometric data. In this case, the company must also collect specific identifying information from the data subject.

Companies must take steps to reasonably secure information and protect its confidentiality.

Cross-border transfers of personal information are restricted to countries that provide adequate protection. If adequate protection does not exist, data may generally only be transferred with the written consent of the data subject or to effect an agreement between the parties.

Companies must provide privacy notices and respect the rights of data subjects, including rights of access and to revoke consents.

The law establishes a data protection authority to enforce the law and ensure the data subjects' rights. Companies must notify this authority regarding their data processing activities. Inter-

estingly, notification is not required for processing a company's own HR data.

Existing databases must comply with the requirements no later than January 1, 2010. However, DPA notification must occur by January 1, 2008.

If you have any questions or would like an unofficial English translation of the law please call Peggy at 404-914-1163.

## Security Programs

mental problems (such as natural disasters or power failures)?

Do you have defined physical security zones? Do you control access within your facilities based on these zones? Do you control environmental contaminants and electronic penetration?

Are all users required to execute appropriate acceptable-use policies and/or non-disclosure agreements?

Are users given access only to information and systems as needed to perform their required functions? Are the access rights adjusted periodically to reflect personnel or system changes? Are users appropriately authenticated, based on the level of risk?

Have you grouped your systems, applications, information and users into secu-

rity domains and set access requirements within and between each security domain? Do you secure your computer networks using multiple layers of access controls? Are your networks appropriately protected using a combination of protocols, filtering routers, firewalls, gateways, proxy servers, and/or physical isolation?

Do you restrict access to operating systems applications and system utilities? Do you monitor access and use? Are operating systems and applications kept current with security patches? Do you use anti-virus products and other filtering technologies to protect against malicious code?

Are applications secured with appropriate time-of-day restrictions and other controls? Do you monitor application usage with software that analyzes user activity patterns?

Do you limit remote access to situations where it is needed for a particular business reason? Do you monitor remote access and secure/isolate remote access devices? Do you use strong authentication and encryption to secure communications?

Do you use encryption to protect sensitive information during transit? During storage? Do you employ effective key management practices?

Are security requirements established prior to development/acquisition of systems and applications? Do you have an effective change control process?

Do you perform appropriate background checks for new employees and onsite contractors? Do you provide security program training to all employees and onsite contractors?

Do you have appropriate media handling controls to protect paper and electronic media? Do you ensure secure disposal of media containing company or personal information?

Do you conduct due diligence on service providers? Do you require contracts that include confidentiality, defined security controls and reporting? Do you audit your service providers? Do you have a process for coordinating incident response?

Do you have processes to respond to an information system intrusion, including the containment and restoration of systems? Do you have a formal incident response plan? Has this plan been tested?

Do you have an established business continuity plan? Do you have sufficient insurance coverage given the identified security risks?

If you have any questions about the legal requirements for information security, please call Peggy at 404-914-1163.

### Insurance Coverage Alert!

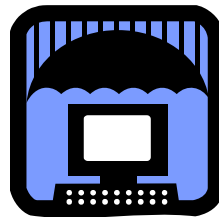
We recently renewed the PIMS general liability insurance policy and received the following IMPORTANT NOTICE from our carrier:

Your Commercial General Liability policy will include a change at renewal or at the next anniversary date as follows:

**Exclusion – Violation Of Statutes That Govern E-Mails, Fax, Phone Calls Or Other Methods Of Sending Material Or Information** will be attached to your policy. This endorsement is an exclusion of bodily injury, property damage and personal and advertising injury arising directly or indirectly out of any action or omission that violates or is alleged to violate the Telephone Consumer Protection Act (TCPA), the CAN-SPAM Act of 2003 (including any amendment of or addition to such laws), or any other statute, ordinance or regulation that prohibits or limits the sending, transmitting, communicating or distribution of material or information.

This is a reduction in coverage in states where, absent the wording of this endorsement, courts would consider coverage to be provided for violations of the above-mentioned acts or of other similar statutes, regulations or ordinances.

Does your insurance policy have a similar exclusion? Given the potential liability associated with marketing programs, we recommend taking steps to ensure that you have sufficient coverage for these types of claims.



This newsletter is intended for clients and friends of Privacy & Information Management Services—Margaret P. Eisenhauer, P.C. PIMS is a Georgia Law Firm specializing in privacy, security and information management. If you do not wish to receive communications from PIMS, please email tanya@privacystudio.com—we will gladly remove you from our mailing list.

The information contained in this newsletter has been prepared for informational purposes only and is not legal advice. This communication is not intended to create an attorney-client relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. If you are not a current client of PIMS, please do not send any confidential information.

Privacy & Information Management Services—Margaret P. Eisenhauer, P.C.  
4355 Cobb Parkway—Suite J-280, Atlanta GA 30339  
Phone: 404-914-1163  
[www.privacystudio.com](http://www.privacystudio.com)