

# The Compliance and Risk Connection

## News You Can Use

February, 2009

Sponsored by...



### Greetings!

Welcome to your edition of The Compliance and Risk Connection. Our objective is to provide compliance, privacy, risk, and security professionals with informative articles, and timely news that will help you in your day to day activities. Each issue features one or more articles from industry experts, and will include news summaries and links to recent information on regulatory changes you need to be aware of, as well as compliance enforcement actions.

We welcome your input. Please send feedback on this publication to [info@aviorcomputing.com](mailto:info@aviorcomputing.com).

Sincerely,

Avior Computing

Copyright 2009, Avior Computing. Avior BenchMark, Avior ClearView, and Avior Computing are Trademarks of Avior Computing Corporation.

## In This Issue

[Regulatory Changes](#)

[Compliance Enforcement News](#)

[Breach News](#)

[Featured Article](#)

## Regulatory Changes



**Red flag provisions:** Although these rules and guidance from the FTC and other financial regulators were put in place some time ago (see [FTC notice](#)), they only took effect Nov. 1, 2008. The rules impact financial organizations of all types, and they add some obligations in terms of oversight of service providers for identity theft detection and prevention. These provisions are pretty interesting in light of the Heartland breach described below. The full text of the red flag provisions is found [here](#).

### Quick Links

**Next Avior Webcast:**  
Feb. 24, 1:30 EST

**"Managed Vendor Risk Service"**

[Register Now](#)

[Avior in the News](#)

### Our Sponsor:

[Avior Website](#)

## Free Assessment and Gap Analysis Offer

Avior Computing is offering a free assessment and GAP analysis using our BenchMark solution. This self-assessment, developed by leading experts on privacy and compliance mapping and based upon GAPP Principal 8 - Security for Privacy - has 57 questions that will help determine the current state of your information security and privacy programs. In addition to providing a snapshot of your current state, Avior's advanced analytics and reporting will

**New Mass. law: [201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth](#)** . This new state law sets a new "high water mark" among state privacy laws, in terms of the degree to which it prescribes specific information security controls. Among the requirements: "Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information", and "Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information". The law also describes specific user authentication, access control, and encryption measures that businesses must undertake. The compliance date for the law was recently pushed back to May 2009.

allow you to compare your organization to other summary (anonymous) findings from other similar organizations. To sign up for this offer, please contact Melinda Thomas at [mthomas@avior.com](mailto:mthomas@avior.com), or [puting.com](http://puting.com), or 603-886-8145, x.107.

## Compliance Enforcement News



**HIPAA:** A little dated (July 08), but noteworthy due to the \$100,000 fine levied against this healthcare provider, and the [Corrective Action Plan](#) put in place for a series of HIPAA violations - [Computerworld article on Providence Health](#).

**Privacy violation:** Delaware insurance commissioner fines a health insurer \$150,000 over privacy violations. The full story is [here](#). The insurer mistakenly disclosed the private medical data of 3,800 individuals. The insurer violated two state insurance regulations: one that prohibits disclosure of "any nonpublic personal financial information about a consumer" and another that requires insurers to have a system to safeguard customer information.

**HIPAA enforcement:** Here's an interesting [resource from CMS](#) that provides summary information about HIPAA reported violations. The report is updated monthly, and lists the number of open and closed enforcement cases. Interesting note- 54 of 392 security enforcement cases have been closed via a corrective action plan, which is probably a lot more than one would think reading security headlines. In addition, 87 security enforcement cases remain open.

## Breach News



**Heartland:** The latest big breach (perhaps the largest involving credit card data yet) has to be Heartland, first reported [here](#). The attackers apparently planted card-sniffing malware on their internal IT systems. Initial reports indicated information on as many as 100 million credit cards may have been lost.

**Monster.com:** The big job search site has experienced another security breach, as reported [here](#). This latest breach follows a breach reported in August, 2008, when 1.3 million records were compromised.

## Featured Article

**Information Privacy, Compliance, and Assessments**

The Internet has increased the value of personally identifiable information (PII), creating new types of privacy regulations and protections for PII. The rapid growth in wireless mobile devices is dramatically increasing the threat to PII.

The value of PII escalates in virtual worlds, with ID thefts by cyber criminals inflicting new levels of damage and abuse perpetuated anonymously across national boundaries. According to the Identity Theft Resource Center ([idtheftcenter.org](http://idtheftcenter.org)) the number of disclosed identity breaches increased by 47% from 2007 to 2008, with 656 publicly disclosed identity breaches resulting in over 35,000,000 records stolen. Citizens also seek protections against abuse of PII by large corporations and governments.

One of the first privacy laws was the European Union Privacy Directive of 1995, which unified and strengthened earlier protections found in various EU nations. Other privacy regulations have been implemented by Canada (Personal Information Protection and Electronic Documents Act, 2004) and privacy initiatives are underway in Japan, China, India and many other countries.

Federal privacy legislation in the U.S. has not established a universal definition of protected information, enforcement role, breach notification, or penalties. Certain PII in healthcare (Health Insurance Portability and Accountability Act, 1996) and consumer finance (Gramm-Leach-Bliley Act, 1999) have been defined, with some protections and enforcement. Federal privacy legislation has helped to raise the visibility of privacy issues described in the Generally Accepted Privacy Principles[1]. The lack of a universal Federal privacy law has led to more than 40 states in the U.S. passing various types of privacy laws[2], with breach notification being most common. The recently enacted Massachusetts law, 201 CMR 17, breaks new ground by specifying numerous administrative and technical security controls to be implemented by organizations that process and store the PII of Massachusetts residents.

### **Privacy Means Compliance and Security**

Privacy is broadly understood but privacy protections are far less widely deployed and enforced. All components of a privacy program are subject to examination by auditors to determine if PII is being properly managed and secured.

### **Effective Privacy Requires Management**

Few organizations do a thorough job of managing privacy, compliance and security. According to a recent global survey of more than 7,000 IT executives, 30% of responses did not have an effective security and compliance program.[3]

This means that few companies can claim to have adequately performed the first step in a privacy compliance program, which is to identify all of the PII they own and maintain, and all of the PII touchpoints in an organization. This includes all of the internal and external networks that communicate PII, systems and applications that process PII, and servers that store PII. Additionally, all users must be properly trained on PII and how to protect it, and their actions with PII must be monitored and logged

### **Privacy Compliance**

Properly complying with privacy regulations usually leads to business adopting a risk management viewpoint. Risk management is a lifecycle that begins with an assessment of vulnerabilities and leads to developing countermeasures for threats that pose an unacceptable level of probability and impact.

Countermeasures begin with written policies detailing the PII or resource, where and how it is used, who is responsible for protecting it, and the scope of protections.

Policies, like business, may change frequently in response to changing conditions. Privacy regulations also specify a role for more detailed written procedures to detail the steps to be taken with systems and processes to enforce the policies.

### **Privacy Controls**

Security controls, also known as policy enforcement points, are the various technologies companies buy and deploy to protect their PII. Sometimes referred to as technical countermeasures, security controls include all of the firewalls, intrusion, malware defenses, logging tools, authentication and access controls systems, and other defenses installed inside or outside an organization.

Security controls represent a significant capital and operational investment for most companies, requiring the commitment of capital and people for many years. Controls, like policies and procedures, frequently change and must be monitored, updated, backed up and replaced, representing a significant lifecycle cost. Companies seeking to reduce the costs of security controls are fueling rapid growth in managed security services.

### **Assessments and Audits**

The entire risk management program for a company owning and managing PII must be periodically assessed and audited by both internal and external experts. Audits typically begin with written policies and procedures, and how they are implemented in the technical controls. Assessments can include penetration testing and often begin with the technical controls. Audits and assessments should focus on all PII touchpoints inside and outside the company.

Privacy audits and assessments can be costly exercises, requiring expensive internal and external resources. Compliance management tools help to streamline privacy programs by automating many of the internal and external audit and assessment tasks. Reducing the time commitments of expensive auditors lessens the cost of a compliance program, including any ensuing remediation to address deficiencies uncovered. Compliance automation tools also can unify overlapping and redundant privacy requirements and map them to policies, procedures and technical controls, to quickly provide audit documentation.

### **Conclusions**

A well-managed privacy program provides significant business benefits by helping to align privacy with compliance and security to support business strategy. Managing privacy policies, procedures and technical controls also helps to accelerate compliance maturity, so that each subsequent assessment, audit or remediation step becomes more efficient and less costly. Specific steps to a well-managed privacy program are efficiently managing:

- Periodic privacy assessments and audits to verify the adequacy of privacy controls enforcing privacy policies
- Redundant and overlapping regulations, and mapping the unified requirements to a common set of security controls
- Internal and external audits and assessments processes to reduce the time and cost

[1]

<http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Generally+Accepted+Privacy+Principles/>

[2] <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>

[3] "Findings: The Global State of Information Security, 2008" Price-Waterhouse-Coopers



.