



accenture

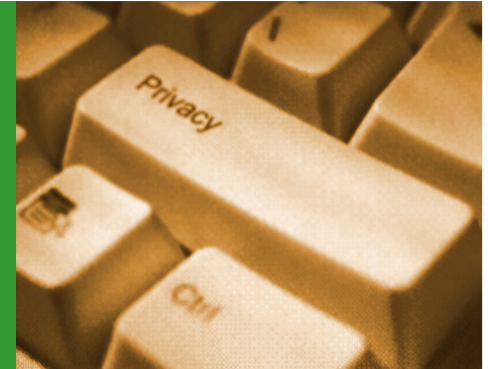
High performance. Delivered.

Security Breach Notification – Reflections on the U.S. Experience



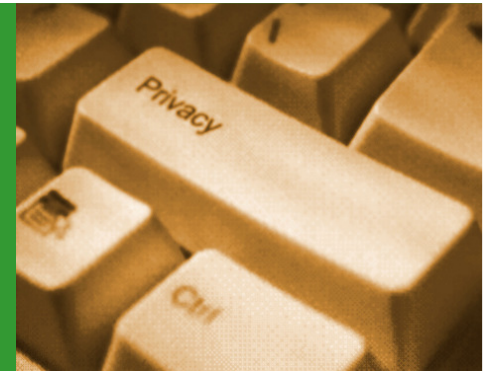
Bojana Bellamy
Director of Data Privacy
Accenture

Brief History of Breach Notification Laws



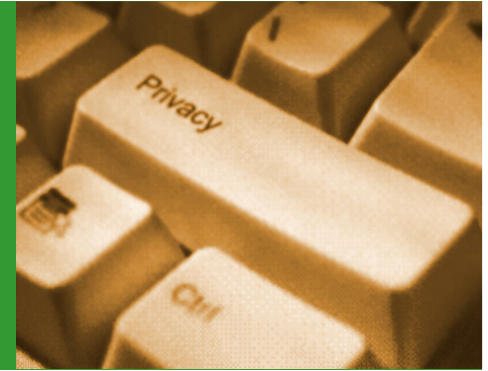
- California passes first security breach notification law in 2003 —“California S.B.1386”
- Following highly publicized data breaches, remainder of US states adopt similar (but at times conflicting) laws by 2008.
- In 2009 the federal health privacy law (HIPAA) is expanded and requires notification of any loss or theft of protected health information - a significant expansion of the specific data that can trigger a notification.
- Canada and Japan follow, with Australia, New Zealand, Hong Kong all proposing breach notification
- Europe – obligation to notify spreads , either by law (Germany, E-Privacy Directive, France, Austria) or by best practice expectation from DP authorities (UK)

Anatomy of a Typical Breach Notification Law (before HIPAA)



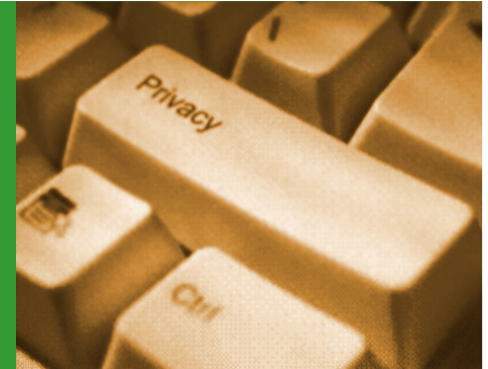
- **Limited data elements** trigger a reportable breach:
 - name+ financial account data, credit card number, national ID or other government-issued ID numbers
 - Basic contact data, CV data, even HR data would not trigger a notification if these other data elements are not present.
 - HIPAA and a California amendment go much further, covering all “health” data - even a list of names is health data when it is a doctor’s list.
- **Event** that triggers notification requirement is “**unauthorized acquisition**” of data.
 - Many state laws and HIPAA require notification only where there is a manifest risk of harm to the affected data subject.
- Notification by data controllers is to affected **individuals**, and in some cases to **regulators**.
 - Data processors are required only to notify the relevant data controller.
- Notification must be made **quickly**. Failure to notify in a timely manner can be basis for legal action.
- **Encryption** is a defense – if the data was encrypted, no notification is required.
- Laws have **extraterritorial** effect – no matter where the breach occurs, the law of the data subject’s home country must be followed.

Lessons Learned--Commercial



- **DP authorities and the public may be surprised to learn how many incidents occur**
 - This surprise will translate into pressure on companies who suffer breaches.
- **Security breach notification laws will have a tremendous effect on commercial discussions and contracting between data controllers and data processors.**
- **Readiness and quick response are essential**
 - A well documented and communicated reporting and response procedure is essential
 - Key people - computer forensics experts, communications, business people with operational knowledge, and lawyers.
 - Managed by trained, experienced personnel.
- **Costs associated with breaches are €35-150 per data record**
 - Costs are often spiraling, often including call centers and credit monitoring services
 - Responses to a breach should be tailored to facts and aimed to restore credibility and prevent further breaches

Lessons Learned -- Legal



- **Including a “risk of harm” trigger in the law is important**
 - Early laws required notification in any case, even if an unauthorized person saw the data). Result was over-notification of data subjects, de-sensitizing them to the risk of a real breach.
- **Encryption is a key defense** – gives companies a tangible path to follow to protect data and themselves.
- **A single breach notification law is preferable** - US likely to adopt a federal law that would pre-empt 50 state laws. Europe should avoid different rules across the Member States.
- **Prevention becomes more important** – focus on data minimisation; finality principle; data being adequate and not excessive; appropriate access and sharing; limited retention;
- **The need to protect data will lead to new conflicts with data privacy requirements**
 - Companies will increasingly need to monitor network, systems, emails and equipment
 - Background checks of employees