itbusiness.ca
Business Advantage through Technology

Print

Alberta's privacy leader makes a case for balance

Alex Campbell tackles the issues of enterprise disclosure and accountability
9/6/2005 5:00:00 PM
by Alex Anderson

In today's world of mouse-click government, data-on-demand and identity theft personal privacy is one of the most sensitive issues facing any large organization, whether in the private or public sectors.

"It's important to strike the best balance between the privacy of the individual and the business goals of the organization. In other words: accomplish what you need to do, but disclose only what you absolutely must," said Alex Campbell at the Government and Health Technologies Forums 2005, held recently in Ottawa.

As executive director for privacy and policy assessment for the Government of Alberta, Campbell led the development and implementation of Alberta's ground-breaking privacy architecture.

Campbell is a firm believer that privacy legislation - Canada has more than 20 laws on the books addressing the private sector, the public sector and the health industry - is not enough on its own to strike that critical balance. Privacy needs to be designed right into the system architecture. Automated systems cannot be effectively managed with manual privacy controls alone, he said.

Addressing a packed session at the conference, Campbell outlined a set of elements that should be included in any privacy architecture.

To start with, any privacy architecture has to be based on privacy standards: Specifically the OECD Data Protection Principles of 1980 and the CSA Model Privacy Code of 1995. Following that there is a set of elements that he said are critical to the foundation of such an architecture:

Following that you have to settle on a lexicon. The tricky thing about vocabulary, especially in technology, is that different people use the same word to refer to different things, said Campbell. For example early planning sessions in the creation of Alberta's architecture tripped over the word 'record.' Thus a clear common terminology needs to be established.

Most systems are based on the separation of data from the elements that link it to a particular person. Social insurance numbers, addresses, licences and names are all identifiers. Any privacy system needs to be able to isolate and control these identifiers.

"The greatest risk to privacy is not malicious actions but inadvertent, accidental disclosure," said Campbell. Identifier isolation mitigates this risk through a couple of methods. One is encryption, which he said can be problematic in long term applications. The other is depersonalization, which separates the identifiers from the attributed records. Instead an internal identifier, such as a meaningless random number, links them. This way, even if information is leaked, it is about File # 2857 instead of John Smith.

It's critical to tackle this element effectively, said Campbell because "it is difficult to manage the sharing of information between different domains unless you can connect it to an identifiable individual."

Privacy transformation refers to the ability to optimize on demand the amount of personal information that is revealed in screens, reports and data warehouses, and thus, achieve a balance between privacy requirements and business objectives.

People have to have the ability to access their own personal information.

"This is one of the most overlooked aspects but one of the most important," said Campbell. "Privacy architecture should provide methods to allow for private access.

This is one of the most challenging elements in privacy architecture. "You don't want to give out this data to

anyone other than the person it regards, so extremely strong access controls are required." Information also needs to be consolidated from different organizations into one access point.

There must be some accountability processes: logs, exception reports and other features to support the legal accountability of the organization. According to Campbell, processes are different in the private and public sectors, but he pointed out a set of common accountability features: privacy impact assessments, security/threat assessments, private access, audit logs and, access control and monitoring.

Privacy metadata must be included to record privacy-related data characteristics and policies.

Finally, policy automation encodes the rules and rules engines to automate routine privacy decisions at the transaction level and minimize time-consuming manual processes that have been the standard.

This is the proverbial 'next step' in privacy architecture, said Campbell. "Nobody has done this yet. The closest anyone has come is P3P - a system included in Web browsers that enables the user to modify how he wants the system to treat cookies.

"When we have applications dealing with high volumes of privacy-sensitive transactions it becomes very difficult to rely on manual processes."

Comment: info@itbusiness.ca

Print

Close Window