

# Data Privacy and Protection



*High performance. Delivered.*

## Alastair MacWilson

Global Managing Director  
Accenture Security

Hi. I'm Alistair MacWilson, the Global Managing Director of Accenture's Security Practice.

Working with the Ponemon Institute, a firm that conducts independent research on privacy, data protection and information security policy, Accenture recently conducted an extensive global survey of more than five thousand business leaders and fifteen thousand individuals across nineteen different countries.

The purpose of this research was to better understand how business practitioners and consumers are responding to growing privacy and data protection threats. To provide some context, issues involving privacy and data protection have long been a sensitive topic for organizations. Now however, a tipping point has been reached. While some organizations have made significant strides in securing their data, others are still lagging behind.

Organizations are contending with the adoption of new technology, new business models and new business processes. Not to mention the volume of data that businesses

• Consulting • Technology • Outsourcing

collect, store and analyze which has all increased exponentially. Data breaches have very serious consequences for organizations today. Not only have punishments and fines increased but breaches can do real damage in terms of reputation, shareholder price and brand.

At a high level five key findings emerged from our research. There's a notable difference between organizations intentions regarding data privacy and how they actually protect it, creating an uneven trust landscape. The study revealed that the majority of companies have lost sensitive personal information with the biggest causes being internal and something they could potentially control. The data shows that many organizations believe complying with existing regulations is sufficient to protect their data but this is a dangerous mindset since regulations generally are not sophisticated enough for today's business environment, nor are they consistently applied across industries and countries.

The survey also underscores the importance of understanding the protection and privacy policies of third party business partners and finally the study revealed that companies that have a more stringent culture with respect to data protection and privacy – what we call a culture of caring – are far less likely to experience security breaches.

These findings as well as our experience with our global clients, lead us to suggest six tangible steps that organizations should take to protect their sensitive data. First, assign ownership and responsibility for data protection and privacy throughout a data governance program. Next, create an information strategy that identifies, tracks and controls how data flows across all areas of an organizations systems and processes. Third, evaluate current data protection and privacy technologies to confirm they're providing the appropriate level of protection. For example, while organizations place a premium on protecting their infrastructure from malware, that won't necessarily protect

the data that employers have stored on their iphones. Fourth, re-examine data protection and privacy investments to ensure they're balanced across people processes and technology. Fifth, carefully choose business partners and maintain high standards when it comes to vetting service providers that handle sensitive data. And lastly, implement formal incident response policies, procedures and teams so that a strategy is in place if something goes wrong.

It's clear that data protection has moved well beyond the technology matter and is now a critical business issue. Organizations that view the issue of data protection and privacy as a C-Suite concern and make it a core principle that guides their business will reap the benefits.

Copyright © 2010 Accenture  
All rights reserved.

Accenture, its logo, and  
High Performance Delivered  
are trademarks of Accenture.