Build customer trust through data privacy

Data privacy is an urgent issue for both consumers and businesses. With each high-profile breach that makes the headlines, customers increasingly worry whether their personal information is protected and being used appropriately. Businesses are also on notice: Recent disclosures about government and corporate practices have pushed privacy to the forefront. With the new Australian Privacy Principles (APP) now in effect since March 14 2014, the enforcement powers and penalties for privacy breaches have never been greater.

But amidst the growing scrutiny, are business leaders looking at the glass half empty? By considering only what privacy safeguards can prevent - customer loss, brand damage, fines, litigation - they miss out on what the right strategy can enable. Customer data is one of your most valuable assets. Companies that not only protect that data but empower customers to have a say in its use build trust in their privacy programs - and their business.

Rethinking privacy is just one key part to keeping pace with today's changing realities. As part of the bigger picture, companies must re-evaluate their approach to cybersecurity, understanding the new threats and opportunities a digital world brings[1].

Why you need privacy they can trust

1. Customers demand it. 89% of consumers say that they avoid doing business with companies that they think do not protect their privacy online[2]. 60% of Australians have decided not to deal with a company due to privacy concerns[3].
2. Investors do too. 85% of investors said boards should be involved in overseeing the risk of compromising customer data[4]. And 61% of directors are engaged in overseeing or understanding data privacy issues. 96% of Australians believe companies should disclose data breaches[3].
3. It impacts the top and bottom lines. A single data breach is costly - more than USD$500,000 on average for companies. Add to that the reputational costs of lost revenue: A breach increases customer churn nearly 4%[6].
4. The personal data ecosystem is here. Services that let consumers decide how their data is used could change how you deal with personal data. One estimate? It could save 10 billion hours annually[7].
5. The retail and consumer sector accounts for 45% of all global data breaches[8].
6. 2013 can be tagged as the "year of the retailer breach", where there has been large-scale attacks on payment card systems[9].

Highlights

Data privacy is becoming instrumental to company growth and brand health; it's no longer solely about managing risk.

Winning consumer trust is where leading organisations focus. Their enhanced privacy efforts often surpass - and may even inform - regulatory requirements.

How you manage data privacy and communicate that in the marketplace can distinguish you as a business that is trusted by customers and other stakeholders.

Understand your data assets, your business and customer priorities, and which privacy frameworks fit your organisation.

For more information, please contact:

Clare Power
Partner
+ 61 3 8603 2360
clare.power@au.pwc.com

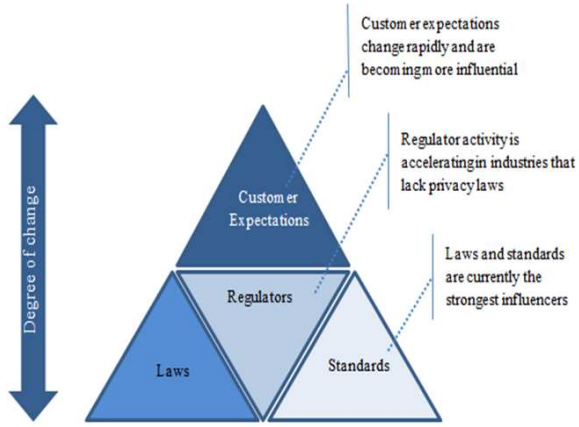
Grace Guinto
Data Protection and Privacy capability lead
+61 3 8603 1344
grace.guinto@au.pwc.com

[1] PwC,10Minutes on the stark realities of cybersecurity, 2013
[2] TRUSTe 2014 U.S.Consumer Confidence index
[3] Office of the Australian Information Commissioner (OAIC), Community Attitudes to Privacy Survey – Research Report 2013
[4] PwC, Annual Corporate Directors' Survey 2013
[5] PwC, 2013 Investor Survey
[6] Ponemon Institute, 2013 Cost of Data Breach Study.
[7] World Economic Forum, 2013 Unlocking the value of personal data
[8] Trustwave, 2013 Global Security Report
[9] Verizon Data, 2013 Breach Investigations Report

Build customer trust through data privacy

Why Privacy is a balancing act

The outside forces influencing your privacy strategy (by degree of change)



Once considered the domain of the legal, compliance or IT functions, data privacy is now an urgent priority for company executives and boards. Regulations under the Australian Privacy Act 1988, for example, are now joined by other high-stakes drivers - revenue and reputation.

It's almost a cliché to be reminded just how vital data is to your business. Whether engaging customers via mobile apps or selling goods in a physical or virtual store, most business activities increasingly rely on customer and other sensitive data. No matter your industry or business priorities, data protection and privacy must be a key part of your growth strategy. Some companies see their privacy teams as internal consultants who work with product teams to think through all of the privacy ramifications. Or look at Google, whose services depend on processing large amounts of data. In the name of transparency, the company launched the Takeout data collection tool, which enables consumers to export their data so that they can see what information Google has about them, and so that they have the ability to port their data to another service if they want to.

Given these uncertainties, many businesses see value in creating sustainable, controls-based privacy programs that are focused on the principles for ensuring compliance with the many data protection and privacy laws, rather than trying to comply in silos.

It all comes back to customer trust

Where consumers set the privacy-trust boundary

What, if anything, might lead you to believe that sharing your personal information has overstepped a privacy boundary?

Learning what customers want, then shaping the business around it, has become a priority for many companies[10].

How to win their trust

At a minimum, customers want to know why you're collecting their data. This means developing proactive processes for considering privacy in the design of products and other business processes that collect or use consumer data, rather than taking a reactive approach to dealing with privacy issues after they emerge.

Honour your commitments

Consumer expectations demand that organisations create an environment of privacy and awareness. What does that really mean? Company leaders have clearly articulated the importance of privacy and that establishing trust with customers at every step of the relationship is good for business. When executives talk and emphasise privacy, organisation-wide awareness improves and so does the customer experience[11]. It also means building privacy practices and controls into business processes that collect, use, or disclose data, so that these commitments become a part of the way the company operates.

Take the lead on trust

A privacy strategy that builds trust starts with these considerations

An important first step is to treat your data the same way you would your financial and physical assets. You need to understand what data you have, what its worth, and who has access to it. All too many companies simply don't have a handle on this.

Where in the world is data privacy headed? Obviously, no one can say for certain. However, it's in the interest of every company to keep an eye on the future. As new technologies appear on the horizon, as legislators start to share new laws, as businesses continues to innovate and push the privacy envelop and as consumers express new concerns about their rights[12] - it would be prudent for companies to continue to build trust with consumers through data privacy.

[10] PwC, 10Minutes on building a customer-centered organisation, 2013
[11] IAPP Privacy Advisor, May 1 2013
[12] International Association of Privacy Professionals (IAPP)

Australian Privacy Principles (APP)

Tips for considering your compliance with the new Privacy Principles

The Office of the Australian Information Commission (OAIC) is responsible for the new Australian Privacy Principles (APPs) effective from 12 March 2014. The new 13 APPs supersede the 10 National Privacy Principles.

The amendments to the APPs give the Information Commissioner enhanced enforcement powers, including the ability to impose civil penalties, accept enforceable undertakings, and conduct privacy performance assessments.

The key changes to the privacy principles include and relate to:

- Privacy policy disclosure requirements, including the complaint handling process and the overseas locations in which personal information (PI) is likely to be disclosed.
- New prescriptive requirements relating to accessible mechanisms for dispute resolution and complaint handling.
- More stringent requirements for direct marketing which will typically require changes in both policy and procedure.
- Cross border disclosures and accountability, including taking a 'reasonable' approach to ensure third parties do not breach Australian APPs.
- Collection and disclosure, which include regulation introduced in dealing with unsolicited personal information and collection of secondary data;.
- Credit reporting, where credit providers can now collect and /or report to Credit Reporting Bodies positive credit data about individuals.

The introduction of the new APPs represent an opportunity for APP entities to build and better manage sound relationships with customers if viewed through a lens of customer privacy protection rather than simply regulatory compliance. Other opportunities to benefit from these changes include:

- Profit from a revised privacy policy which is more customer friendly and transparent.
- Gaining access to a broader range of information to assist in establishing credit worthiness.
- Use of information collected for outsourcing, vendor management and offshore purposes.

Some challenges we have seen within organisations relate to:

- Identifying all their third parties vendors and understanding where they store PI.
- Inventory of all PI collection forms that require updating to inform customers of the privacy arrangements.
- Policies and processes around the destruction or de-identification of PI when it is no longer required.

The areas in which we are assisting clients include determining whether existing practices, systems and processes are in compliance with the APPs or need to be changed. While the APPs have come into effect, many organisations are still working through the details to bring their practices into alignment. Hence, post implementation reviews are being used to validate privacy approaches.

For more information, please contact:

Dante Peel
Partner, Risk Services
+ 61 3 8603 2018
dante.peel@au.pwc.com

Nicole Salimbeni
Partner, Risk Services
+61 2 8266 1729
nicole.salimbeni@au.pwc.com

www.pwc.com.au/industry/retail-consumer

Retail & Consumer contacts:

Stuart Harker
Australian Retail & Consumer Goods Consulting Leader
Global Retail & Consumer Goods Advisory Leader
+61 3 8603 3380
+61 418 339 231
stuart.harker@au.pwc.com

Australia:

John Riccio
National Digital Change Leader
+61 3 8603 4968
+ 61 419 275 097
john.riccio@au.pwc.com

Paddy Carney
Partner
Assurance
+61 2 8266 7312
paddy.carney@au.pwc.com

Lisa Harker
Partner
Assurance
+61 3 8603 2147
lisa.harker@au.pwc.com

New Zealand:
Julian Prior
Partner
+64 9 355 8591
julian.m.prior@nz.pwc.com

Peter Konidaris
Partner
Specialist Taxes and National
Business to Consumer Leader
+61 3 8603 1168
peter.konidaris@au.pwc.com

Suzi Russell
Partner
Specialist Tax
+61 2 8266 1057
suzi.russell@au.pwc.com

Sarah Saville
Partner
Corporate Tax
+61 2 8266 8665
sarah.saville@au.pwc.com

Daniel Rosenberg
Partner
Private Clients
+61 3 8603 3886
daniel.rosenberg@au.pwc.com

Kate Warwick
Partner
Advisory
+ 61 3 8603 3289
kate.warwick@au.pwc.com

If you have any feedback for us, or if there are any topics or issues you would like to see in upcoming editions, please contact:

Stuart Harker
+ 61 3 8603 3380
+ 61 418 339 231
stuart.harker@au.pwc.com

Andrea Marffy
R&C Industry Manager
+ 61 3 8603 3245
andrea.marffy@au.pwc.com