Trust starts from within
Deloitte Australian Privacy Index 2017
“The (recent) significant evolution in data collection and analysis ... suggests that the culture, standards and policy structures that have been applied to big data analytics, may need to move out of the back room and into the showroom, if community confidence and wide opportunity for innovation are to be maximised.”

Timothy Pilgrim, Australian Privacy Commissioner, ‘Privacy, Data & De-identification’ (CeBIT, Sydney, May 2016)
Introduction

In this third Annual Privacy Index, Deloitte seeks to assess the difference between what an organisation thinks it is doing versus what staff believe is actually occurring when it comes to protecting data and honouring customer privacy.

We surveyed ASX 100 companies in conjunction with leading consumer brands in the Australian market. Over 1000 consumers responded to the consumer survey.

We found the dichotomy that can exist within organisations, between governance and operational practices, is often ignored. An organisation may, for example, feel it has ticked the requisite boxes and has all its policies and procedures in place. Yet staff members may circumvent these processes, finding easier ways of doing things – even if ‘adequate’ monitoring processes are in place.

**Trust comes from within**

It is worth remembering that employees and contractors are consumers of other organisations. Thus, they are becoming increasingly aware of what may or may not be done with their information, through their experiences in the organisation they work for.

Positive information handling practices give individuals, such as employees, confidence. These individuals then translate into consumers with an inherent level of trust.

Poor or unethical information handling practices however can cause people to both lose trust with the organisation they work for and treat other organisations with suspicion when providing information.

As all organisations exist in this dynamic landscape – all can lose out. To stand out from the rest, Deloitte has found a sustainable answer which is to build trust from within.

This creates a more capable, educated and confident business community comprised of organisations, their consumers, policy makers and regulators.

**Privacy-aware risk culture**

As organisations are increasingly under pressure from an ever evolving digital, connected and innovating world, consumer behaviour is changing.

It is in fact changing faster than organisations can keep pace with. Consumers are trying out new technologies and, consequently, becoming exposed to new risks; risks which may well take an organisation by surprise.

Increasingly, consumers are carrying these new technologies into their work environment. In our experience, we also mostly find that staff members are unaware of the potential risks their actions may be introducing to the organisation.

As a result, organisations must ensure they develop adequate policies, procedures and controls to prevent these new and evolving risks being introduced.

*How does one promote a risk-aware culture in your organisation?*

**Deloitte Privacy Index 2017**

Over the next couple of years, the information risk that organisational staff and third parties present to an organisation will increasingly blur the lines between work and play.

This Index aims to shed light on these blurred lines and offer tangible examples of where the risks lie and what to do about them.

Our aim is to inspire your organisation to take a deeper look into its culture and operational processes, and identify behaviours, controls and metrics that better manage your privacy risks.
About this report

The Deloitte Australian Privacy Index 2017 analyses the state of privacy in Australia’s leading consumer brands and the ASX 100 across 11 sectors – consumer/retail, education, energy and utilities, financial, government, health care, industrials, information technology, materials, real estate and telecommunications and media.

Most organisations have reached a level of maturity wherein their policies on website privacy, website security controls and mobile apps are open and transparent to consumers. For this reason, our focus in 2017 was to compare organisational privacy practices with the practices of consumers working in these leading Australian consumer brands and the ASX 100.

The Index comprises a consumer survey of more than 1000 Australian consumers and a confidential organisational survey.

Brand analysis
As in previous years, the internal privacy practices questions assessed how policies and procedures were implemented, and what training, organisational roles, data breach notification processes and privacy awareness initiatives were run both internally and externally. We also included questions on the preparedness of organisations to respond to global regulatory change.

This year, we added questions to delve deeper into the culture of the organisation to gain a better understanding of why privacy is important to the organisation. To understand this perspective, we asked questions to determine the drivers behind the importance of privacy to the organisation, and whether the organisation felt it could do more to protect personal information.

Consumer sentiment analysis
More than 1000 Australian consumers were asked to share their opinions of privacy with a particular focus on trust, complaints and information handling expectations. These consumers were employees of leading Australian consumer brands and ASX 100 companies.

This year, we added a new component to the survey to test consumer attitudes to privacy outside work versus dealing with personal or employee information at work.

The caveat is that Deloitte cannot warrant the accuracy of the information gathered nor the extent it may reflect the reality within an organisation as no testing was performed to verify it at any of the organisations. Circumstances might also have changed over the period of time this information was gathered.

All responses are confidential and only aggregate responses have been reported. Deloitte has compiled the information into a series of graphs. The conclusions drawn about the state of privacy are based on a weighting that was allocated to each of the survey responses and the components considered for the industry ranking.

We would like to thank the following for their support, and for sharing their views and expertise:

- All participating brands in the Deloitte Australian Privacy Index 2017 Survey
- The brands which have continually supported the Index since it commenced three years ago.
# Privacy Index 2017

<table>
<thead>
<tr>
<th>Sector</th>
<th>Rank 2017</th>
<th>Rank 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Government</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Telecommunication and media</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Energy and utilities</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Industrials</td>
<td>5</td>
<td>N/A</td>
</tr>
<tr>
<td>Health care</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>Consumer/retail</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>Real estate</td>
<td>8</td>
<td>13</td>
</tr>
<tr>
<td>Information technology operations</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Materials</td>
<td>10</td>
<td>N/A</td>
</tr>
<tr>
<td>Education</td>
<td>11</td>
<td>6</td>
</tr>
</tbody>
</table>

- ![Increased from 2016](image)
- ![Not ranked in 2016](image)
- ![Decreased from 2016](image)
- ![No change from 2016](image)
Executive summary

Organisations are facing growing pressure from emerging privacy and data protection regulation locally and globally – hence the focus on compliance ahead of building trust with consumers.

The good news is that the regulation that is emerging is consumer-centric and encourages transparency.

The Index reveals the overall ranking of 11 industry sectors.

Key themes

- Privacy and data protection are not seen as inhibitors to innovation or customer experience
- Organisations believe they can do more to protect information about customers and employees
- Compliance stands out as the main driver behind current privacy and data protection practices, ahead of building trust with customers.

Overall sector ranking

This year, the list demonstrates how industries performed according to consumer expectations as well as whether they exhibit good privacy practice. Indicators assessed included:

- The drivers behind current privacy practices within organisations
- Do controls implemented translate into compliant behaviours
- To what extent employees, as consumers, trust their own organisations
- Security measures within organisations
- Preparedness for regulatory change
- For the second consecutive year, the financial industries surpassed government as leaders in privacy.

Key insights

- The top three industries are all highly regulated with respect to privacy and data protection risk
- 54% of organisations manage third party compliance with privacy obligations upon contract review only, 21% of organisations do not do anything at all
- Email is still widely used for workflow involving personal information, especially to and from third parties
- Training and policies do not necessarily translate into compliant behaviour
- 58% of employees in organisations believe being legally compliant is the primary reason privacy is important to their organisation.

Synergies between the brand and consumer surveys

Building trust

While most organisations that completed the brand survey agreed that building trust with consumers is a competitive advantage, their staff revealed that being legally compliant was still the main perceived reason privacy was significant.

This was confirmed by organisations indicating that the driver behind the development of their privacy strategy was to comply with regulatory requirements as opposed to building trust.

Data breach response plan

A poor information risk culture can lead to greater levels of risk-taking. All respondents from the telecommunications and media industry stated that their organisation had a data breach response plan. However, only 43% of respondents from the consumer survey, of which 37% work in that industry, are aware of such a plan.

Misuse or unauthorised disclosure of information

Most organisations that participated in the brand survey revealed that they were confident that their staff would feel comfortable in reporting misused or improperly disclosed information.

This was confirmed in the consumer survey where 93% of respondents said they would report the issue if a customer’s information was used or disclosed inappropriately.

Industries that did well...

- Have internal privacy training that occurs almost annually
- Require contracted third parties to notify the organisation in the event of a likely data breach
- Had an appointed Privacy Officer role within their organisation
- Conducted formal privacy impact assessment for each significant change
- Published privacy awareness or education materials internally in the last 12 months
- In particular, the financial industry did well because organisations in this industry conducted frequent privacy training and their employees could correctly identify what a privacy impact assessment was and the process to follow in the event of a data breach
- Have employees that would be comfortable being consumers of the brand they work for.
At a glance

Brand survey

While the focus for organisations is compliance, are they neglecting building trust with...

... consumers?

- 36%
- 32%
- 4%

... employees?

- 23%
- 18%
- 59%

Organisations believe they can be more transparent with consumers about how their information is used.

- 91%
- 5%
- 4%

The top three industries seen by consumers to exhibit practices that lead to trust are...

- Government
- Financial
- Telecommunications and media

The three industries seen by consumers to exhibit practices that do not always lead to trust are...

- Education
- Consumer/retail
- Materials

43% of respondents did not know if their organisation had a data breach procedure, with the majority of responses coming from...

- Education
- Health care
- Consumer/retail

Consumers are most concerned with sharing the following types of information...

- Identification numbers: 69%
- Financial history: 53%
- Fingerprint or facial image: 48%
Brand analysis
Brand analysis

While brands are fostering strong relationships with their employees and customers, building trust is still secondary to being legally compliant. This is due to the growing regulatory pressure locally and globally that organisations are required to comply with.

**Key statistics**
The following list ranks the organisations with a positive risk culture as identified by the organisations themselves (from strongest to weakest):

1. Telecommunications and media
2. Government
3. Financial
4. Energy and utilities
5. Consumer/retail
6. Industrials
7. Real estate
8. Health care.

No responses were received from:
- Information technology operations
- Materials
- Education.

**Privacy strategy**
- 58% of organisations indicated that their organisation has undertaken a formal exercise to develop a privacy strategy
- Of those, 71% indicated that they have refreshed their strategy in the last 12 months
- 46% of organisations have EU customers, of which 18% have not considered how global changes like the EU GDPR will impact their organisation
- The financial industry is leading the way in recognising the impact of the EU GDPR
- 55% of organisations monitor the retention periods for the personal information they hold.

Of the organisations that have a privacy strategy, the primary focus for developing this strategy was:

- Regulatory compliance (43%)
- Building trust with customers (57%)

**Participation in Privacy Awareness Week**
- 54% of brands formally participate in Privacy Awareness Week
- Organisations tend to run internal campaigns that focus on awareness raising among employees. This includes internal awareness campaigns via multimedia.

**Internal privacy training and awareness**
- 88% of organisations indicated they have internal privacy training
- Of the organisations that conduct internal privacy training, 71% conduct privacy training annually
- 75% of the organisations have published privacy awareness and education materials in the last 12 months.

**Privacy metrics**
- 46% of organisations report privacy metrics to the board
- These metrics include the number and nature of incidents and breaches, and training completion.
How often does your organisation review contracted third parties to ensure they are compliant with your organisation’s privacy requirements?

- On contract review: 54%
- We don’t review them: 21%
- Only at the start of the contract: 13%
- Every 2 years: 8%
- When a breach occurs: 4%

Third party management
- 25% of organisations indicated that they were either unsure, or did not require contracted third parties to notify them in the event of a data breach.
- All respondents in the telecommunications and media and government sectors, indicated that contracted third parties are required to notify the organisation of a data breach.

Data breach reporting
- 88% of organisations indicated that their staff members would feel comfortable reporting misused or improperly disclosed customer or employer information.

Data breach response plan
- 79% of the organisations indicated they have a data breach response plan that could be enacted in the event of a significant/critical incident.

Economics and privacy
- 94% of organisations felt that having privacy obligations either did not impact or positively impacted on customer user experience.
- 92% of organisations indicated that building trust with their customers was a competitive advantage.
- There is an opportunity for organisations to reframe the way privacy is perceived – from a regulatory burden to a competitive advantage.

Brand sentiment towards transparency
- 96% of organisations indicated that they would be comfortable telling their customers exactly how their data was being used.

Not all organisations invited to participate in the survey responded to the survey.
Where does privacy sit in your organisation?

- Compliance: 38%
- Marketing: 8%
- Security: 28%
- Other: 8%
- Legal: 4%
- Risk: 4%
- IT: 4%

Does your organisation have a process in place that captures and assesses all privacy related incidents and data breaches?

- 79% of the organisations indicated they have a data breach response plan that could be enacted in the event of a significant/critical incident. Of these:
  - Capture all incidents and breaches, big and small: 50%
  - Capture serious incidents and breaches only: 29%
  - Capture and assess incidents in an ad hoc way or as they arise: 13%
  - Have no process in place to assess: 8%

Privacy impact assessments (PIA)

Leading industries
- Financial
- Government
- Telecommunications and media

Who conducts Privacy Impact Assessments?
- Privacy personnel: 46%
- Manager and staff: 33%
- We do not do PIAs: 21%

Of organisations indicated that they do not have a formal privacy impact assessment process for business changes.

All participants from the telecommunication and media industry indicated they conducted a PIA for business changes.

No brands indicated that their Privacy Impact Assessments were either too lengthy or complicated.

All brands from the consumer/retail industry indicated they did not have a formal process to conduct PIA for business changes.
Consumer sentiment analysis
Trust starts from within

Staff in organisations are consumers too. Organisations need to be more proactive so that consumer behaviours do not translate into risks for the organisation.

Industry ranking
The following list of industries indicate how consumers working in that specific industry perceive the strength of its privacy risk culture (from strongest to weakest):
1. Financial
2. Government
3. Telecommunication and media
4. Energy and utilities
5. Information technology organisations
6. Health care
7. Industrials
8. Real estate
9. Materials
10. Consumer/retail
11. Education.

Number of records of personal information, including customer or employee information dealt on a typical day by the respondents

- 4% are dealing with 1000 or more records
- 8% are dealing with 101-999 records
- 88% of respondents are dealing with up to 100 records

- Of the 88% dealing with up to 100 records a day, government, education and health care are the top three, making up a third of these respondents
- Of the 4% that are dealing with 1000 or more records a day, 25% were part of information technology organisations and 18% were part of the consumer/retail industry.

We surveyed individuals employed across these 11 industries to see if behaviours outside work translated to risks within their organisation.

The participants we surveyed held the following roles:

- Board member
- Chief executive group
- Director
- Manager
- Professional services provider
- Analyst/Developer/Policy officer
- Customer service
- Support services
- Other

Consumer sentiment analysis
Work versus home
- While 79% of respondents had never let someone at work use their work login and password, 41% of these respondents would trust their colleagues to do the right thing if they did choose to share it. The top three industries where respondents would do this were:
  1. Government
  2. Education
  3. Health care.
- While 86% of respondents use up to 40 websites that require a password, 65% use up to only nine passwords across these websites, showing that respondents are using the same password across multiple sites. These employees are at risk of doing the same at work. They predominantly come from health care, education, and consumer/retail industries.
- 47% of respondents share passwords at home, which is more than those who share passwords at work (21%).

Privacy in practice
- 30% of individuals revealed that they share customer or human resources information with other organisations as part of their role. This is how respondents typically share information with other organisations:
  - Email: 66%
  - Other: 57%
  - Verbal communication: 40%
  - Secure file transfer including via a portal: 27%
  - Physical media - e.g. USB or DVD: 23%
  - Insecure electronic file transfer: 22%
  - Hard copy files or letters: 9%
- Email was the most common mechanism for sharing information with other organisations across the following sectors:
  - Government
  - Health care
  - Financial
- 79% of respondents understand it is their responsibility to verify if an employee’s request for customer information is valid, before disclosing information.

Information risk culture
- 58% of respondents believed that privacy was important to the organisation because it is a law they needed to comply with.
- While 92% of respondents stated that they understood their organisation’s privacy policy, 26% revealed that they do not receive training in their organisation’s privacy obligations. Those respondents that do not receive training typically come from Consumer/retail and Information Technology organisations.

The importance of leading by example
- 93% of respondents said they would make a report if a customer’s information was being used or disclosed inappropriately at work. Of these respondents, 66% said they would report this to their Manager. This reveals the importance of the role managers play in identifying and escalating potential breaches.

In the event of a breach, who would you report to?
- 66% The security team
- 13% My manager
- 12% Privacy offer
- 5% Legal/compliance
- 4% Other
- 1% Other

- 7% would not report or were unsure if they would report information that was being inappropriately used or disclosed.
- 49% of respondents received annual training in their organisation’s privacy obligations.
- 43% of respondents did not know if their organisation had a data breach procedure, with the majority of responses coming from the industries below:
  1. Education
  2. Health care
  3. Consumer/retail.
- While 91% of respondents revealed that they would be comfortable being a customer of their own organisation, 9% were not comfortable or were unsure.
Respondents believe that privacy is important to the organisation because:

- It is a law we need to comply with: 58%
- It is personal information and we want our customers and employees to trust us: 36%
- We have to comply with our policies: 5%
- Privacy isn’t important to our organisation: 1%

The top 5 industries in which it was revealed that staff would share their login and password with colleagues because they trust them to do the right thing:

1. Government
2. Education
3. Health care
4. Financial
5. Consumer/retail

The reasons why employees cited they would not be comfortable being a customer of their own organisation included:

- I don’t have privacy training, yet I handle sensitive matters.
- I see breaches happening regularly.
- If the company shares information with third parties, then to me it’s not safe sharing my information with it.
- I know how loosely managed it is.
- Data retention and destruction are very unclear, particularly with email trails.
- Customers can openly see other client’s personal information by simply looking at the screen right in front of them.
- We know that staff from time to time trawl through records.
- Managers have access that they don’t need.
- People are not really appropriately trained in how to handle sensitive information.
- The use and sharing of information processes are often vague internally.
- While in principle the data privacy practices are great, on a day-to-day basis, with less management, these practices are often overlooked in order to be more ‘efficient’.
- Not everyone follows the procedures.
- If the company shares information with third parties, then to me it’s not safe sharing my information with it.
- The use and sharing of information processes are often vague internally.
“Simply put, a successful data-driven economy needs a strong foundation in privacy ... When there is transparency in how personal information is used, it gives individuals clarity, choice and confidence that their privacy rights are being respected.”

Timothy Pilgrim, Australian Privacy Commissioner, ‘Commissioner Welcome: Data sharing and interoperability workshop, GovInnovate’ (Speech delivered at the Crowne Plaza Canberra, 16 November 2016)
Looking forward

In light of emerging local and global regulations, can organisations continue to maintain trust, resilience and confidence while adjusting their business models?

**Who owns data about an individual?**
The Australian Productivity Commission is calling for individuals to have greater control over the collection and sharing of their data.¹

In other parts of the world including the European Union, similar provisions have already been enacted in the Revised Payment Services Directive (PSD2)² and the General Data Protection Regulations (GDPR).³

- PSD2: Retail banking will be disrupted in 2018. The revised directive puts control of access to data held by traditional banks into the hands of consumers. Consumers will be able to choose where they make payments from and banks will be required to provide access to third parties to enable this to occur.

- GDPR: The GDPR enables individuals to request their data in a machine readable format and provide it, or ask the organisation to provide it to another organisation, potentially a competitor.

There are four key challenges organisations with traditional business models and legacy systems are facing:

1. **Organisations need to share risk management with consumers.** Individuals should be able to access information about themselves, control how it is collected, and opt out of sharing it with third parties. To build trust, organisations will need to consider how best to enable consumers to have control of the risk, and monitor any interactions. Yet in the event of an issue, the organisation maintains control and evidence of interactions.

2. **Organisations can no longer be fortresses.** Ensuring essential or requested information is provided via open Application Programming Interfaces (APIs)⁴ to recipient organisations will require organisations to ensure all externally facing changes undergo a privacy impact and/or security assessment.

3. **Risk culture needs to be unassuming.** Bundled consent, Terms & Conditions or Privacy Policies cannot be relied on for management of information. Effective awareness programs within organisations will be paramount, especially where staff members’ unauthorised access to information is monitored.

4. **Potential higher operational costs.** Putting risk in the hands of consumers and third parties means organisations need to maintain control to manage such risk. Organisations will need to ensure they provide both external and internal education programs to answer any questions or manage any surprises from consumers.

By addressing these challenges, organisations can:

- Lower operational costs through reduced calls, questions and complaints, as risk is shared with the customer
- Move from a knowledge-based to a behavioural-based risk culture that is held to account by customers
- Achieve competitive advantage by adopting regulatory changes as a complementary service to customers.

It has never been more important to ensure that the basics are right to maintain consumer trust.

⁴ APIs are sets of requirements that allow one application to communicate with another.
Trust starts from within

Organisations are subject to obligations that require them to notify consumers as to how information is collected, used and shared, and which third parties are involved in these activities. In some cases, organisations choose the bare minimum requirements to satisfy compliance with the obligations.

With the introduction of data breach notification laws such as those in Australia and the EU GDPR, organisations may now:

- Be instructed to notify customers of a breach within a certain time frame
- Be required to expose poor privacy and data protection practices to customers, the regulators, advocacy groups and the media
- Be exposed by third parties to customers, regulators, media or advocacy groups.

While considering bare minimum compliance may be the easiest and seemingly least expensive approach to managing external perceptions, data breach notifications laws mean that risk exposure is increased from an organisation managing a breach internally (in some cases with a regulator), to potentially include third parties, the media, advocacy groups, insurance companies and other authorities that may question internal practices.

By being more transparent, organisations can:

- Further build trust with customers as there are no surprises. Align an individual’s expectations with what is being communicated. This is especially important in the event of a complaint or incident
- Maintain their bottom line, as customers that trust an organisation are unlikely to walk away.

Regulations compelling organisations to open their data will expose how organisations use information and to whom it is provided.

46% of organisations have European citizens as customers. Of these, 82% have considered how the EU GDPR will impact their organisation.

91% of consumers said they would be comfortable being a customer of their own organisation.

Don’t get caught out

- Do your staff members know what content is provided to individuals via notifications and privacy policies?
- How do you monitor how you use and share the data you collect and store?
- How do you know which third parties receive your data and whether they use it in line with your expectations?
- How do you manage your third parties and ensure that your third parties notify you in the event of a breach?
- Can you map the activities your organisation performs with data against the notifications that a customer receives?
Creating a sustainable privacy and data protection program

There has been increased activity in the privacy and data protection landscape over the last 12 months through:

- Proactive regulators
- The impact of privacy and data protection regulations outside the territorial jurisdiction in which they were introduced
- New technology with new risks including virtual reality, artificial intelligence, big data analytics, internet of things, APIs
- Increasing consumer awareness of risks leading to a change in behaviour, such as providing inaccurate information or not providing information at all.

These drivers will not cease in the next 12 months or beyond. In fact, we believe they are likely to become more apparent.

While organisations already have good practices in place including privacy strategy steering committees, user access management, documented policies and procedures, training and awareness programs, and internal audit plans that include privacy and data protection – these activities are largely conducted in isolation from each other with little or no governance or coordination. These activities also tend to be driven by compliance rather than a desire to protect the individual – which is the reason the regulation exists in the first place.

Kinds of information that organisations are using to promote privacy awareness:

- Training materials
- Guidelines
- All staff emails
- Blog posts
- Videos

Organisations may need to consider new processes to manage new risks including:

- Assisting senior management to understand new information risks by aligning risks to the organisation’s objectives
- Appointing a data protection officer (required by some jurisdictions such as the European Union and the Philippines) to oversee and manage the program
- Ongoing monitoring and assessment of the risk of global regulatory changes and decisions made by regulators
- Implementing privacy-by-design thinking to all staff members with exposure to personal information, to foster a positive risk awareness culture
- Monitoring access to data even if access is legitimate, in order to track potential misuse.

For organisations to have confidence in their privacy and data protection practices, a holistic and streamlined approach is necessary to manage this risk.

Of the organisations that have a privacy strategy, a primary focus for developing this strategy is:

- Regulatory compliance (43%)
- Building trust with customers (57%)

Don't get caught out

- Is privacy a compliance requirement or used to build trust with customers in your organisation?
- Do your Board and senior management consider privacy and data protection risk an important part of strategy to grow the organisation?
- What is your approach to privacy and data protection management? Do you have siloed teams working on various initiatives, or do you have a centralised governance approach?
- How often do you conduct a privacy health check on high risk product areas?
- How do you monitor local and global changes to privacy and data protection regulations that may impact your organisation?
- How do you assess the risk presented by your external third parties to privacy and data protection expectations?
- How do you measure the success of your program each year?
Increasing insider threat

‘Insider threat’ has commonly been referred to as the risk posed by staff members from the misuse, unauthorised access or disclosure of information even if the individual has legitimate access to that information as part of their role.

In some cases, employees will have legitimate access to information, however they may also access an individual’s record, or even their own, without a legitimate business need. Further, that information can then be used or shared for a purpose that is not in line with business rules, intentionally or unintentionally. This is one way in which it is evident that training programs, while crucial in educating and changing behaviours, are not always an effective control in monitoring misuses, unauthorised access and disclosure of information.

As well as detective controls, supportive leadership and a positive culture are required to differentiate between legitimate and unauthorised employee and third party access to information. Where this is the case, organisations need to know that employees and third parties may require a privacy notice, and that expectations regarding this monitoring are managed. This will ensure employees understand what will be monitored, and what the consequences might be should a breach be identified.

Don’t get caught out

- Do you monitor unauthorised access, use or disclosure of information by employees or third parties?
- How do you manage employee and third party expectations around monitoring?
- Do your teams work together to identify any misuse of information to which staff members have access?

Percentage of organisations that use the following methods to protect information:

- Policies and procedures: 96%
- Encrypt information sent: 79%
- Mandatory privacy training: 79%
- Encrypt information stored: 75%
- External threat monitoring: 75%
- Identify and access management solution: 75%
- Mobile device management – monitor information leaving the organisation: 71%
- Right to audit clauses in contracts: 67%
- Anonymisation or de-identification processes: 67%
- Internal threat monitoring: 63%
- Issue corporate mobile devices to staff: 63%
- Program building a positive privacy culture: 58%
- Data leakage protection – monitor information leaving the organisation: 58%
- Multi-factor authentication: 54%
- Consent/secondary purpose management: 50%
- Data minimisation: 38%
- Double/triple blindness: 8%
“... our businesses, governments and families are acutely aware of the challenging times that have hit the globe over the past decade: not only economic and political developments, but also the rise of disruptive new technologies and increasing regulatory reach.”

*Building the Lucky Country #6,*

What’s over the horizon? Recognising opportunity in uncertainty
How well do you understand your consumer information risk exposure?

Policies and procedures are no longer sound indicators of behaviour within organisations. Culture and behaviour by staff members, third parties and contractors are exposing new threats coming from within an organisation. The increasing development of global and local regulation has the power to both educate consumers and pose a critical risk that needs to be appropriately managed internally and externally with regulators, the public and the media.

How **confidently** do you understand your customer information risk exposure?

1. For each indicator below, circle the number that indicates how **confident** you are that your organisation actively performs these activities.

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Confidence scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our staff members follow processes and procedures – workarounds are not in our culture.</td>
<td>1    2    3    4    5</td>
</tr>
<tr>
<td>We report metrics regarding information risk to our Board.</td>
<td>1    2    3    4    5</td>
</tr>
<tr>
<td>We could tell any customer how we handle their information.</td>
<td>1    2    3    4    5</td>
</tr>
<tr>
<td>We collect only the information that we need.</td>
<td>1    2    3    4    5</td>
</tr>
<tr>
<td>We generate and keep only the information about a customer that we need.</td>
<td>1    2    3    4    5</td>
</tr>
<tr>
<td>We assess the risk of re-identifying de-identified data sets.</td>
<td>1    2    3    4    5</td>
</tr>
<tr>
<td>We can provide all the information a customer requests about themselves.</td>
<td>1    2    3    4    5</td>
</tr>
<tr>
<td>We monitor new regulations or standards and assess our risk exposure.</td>
<td>1    2    3    4    5</td>
</tr>
<tr>
<td>We adequately monitor misuse of information by our staff members, third parties and contractors.</td>
<td>1    2    3    4    5</td>
</tr>
<tr>
<td>We monitor unauthorised access to information by internal and external parties.</td>
<td>1    2    3    4    5</td>
</tr>
</tbody>
</table>

2. Add up all the numbers circled to determine your overall score and your next step.

<table>
<thead>
<tr>
<th>Score range</th>
<th>Next step</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>45-50</strong></td>
<td><strong>You understand your organisation well! Would your customers and staff members think the same?</strong>&lt;br&gt;Take this exercise to your team and see if you receive similar scores and ensure you have a privacy and data protection review in your audit plan to monitor this risk.</td>
</tr>
<tr>
<td><strong>35-44</strong></td>
<td><strong>Most organisations will fit in here. However, incidents and breaches don’t discriminate. They can occur in the unlikeliest of times in the unlikeliest of circumstances.</strong>&lt;br&gt;Consider how effective your communication with your staff teams is regarding your obligations. Does this translate into their correct behaviour?</td>
</tr>
<tr>
<td><strong>Below 35</strong></td>
<td><strong>People are the biggest threat in organisations.</strong>&lt;br&gt;Consider performing a privacy and data protection health check to understand the areas where customer information risk exposure is the highest.</td>
</tr>
</tbody>
</table>
Methodology

The Deloitte Australian Privacy Index 2017 is the result of analysing Australia’s leading consumer brands including the ASX 100. It is an annual report that measures the state of privacy across 11 sectors.

The input for the Deloitte Australian Privacy Index 2017 report comprises of:
1. A survey of the sentiments of more than 1000 Australian consumers towards privacy, and
2. A confidential organisational survey.

Consumer sentiment analysis

An external organisation, Roy Morgan Research, was engaged to survey more than 1000 Australian consumers to share their opinions of privacy with a particular focus on trust and complaints.

This year, to be able to compare risk behaviour at work versus in a consumer’s free time, participants were selected if they worked for any of the ASX 100 industries or leading consumer brands.

Brand survey

Individuals responsible for privacy risk within organisations were invited to complete a survey on behalf of their organisation. For the first time in 2017, survey results contributed to the overall score for an industry. This is due to the maturity of organisations managing privacy and data protection risk.

Where there was no industry participation, this industry did not receive a score for this component of the Index.

Overall Index result

The overall score and Index ranking comprised of organisation survey results and consumer sentiment analysis.
“Organisations can no longer have a set and forget mentality. Policies and procedures are one thing – behaviour is another. We have reached a point where the introduction of new digital technologies requires active monitoring of consumer information risk exposure. This will prepare organisations for a resilient privacy and data protection program that can sustain evolving expectations from both consumers and Regulators.”

Marta Ganko, National Privacy and Data Protection Lead, Cyber Risk Services, Deloitte
About the series

Trust starts from within

Trust is critical to the success and growth of the Australian economy. As technology continues to evolve and drive commercial opportunities, maintaining trust and loyalty is a key competitive advantage.

The Deloitte Australian Privacy Index series sets out to contribute to the growth of the Australian economy. It is Deloitte’s commitment to assist organisations to build trust with the Australian community in this fast-paced world.

Transparency is opportunity (2015)

Trust without borders (2016)

Trust starts from within (2017)

Other publications you may be interested in:

Building trust across cultures (Asia Pacific)

Voice of Asia (2017)

Beneath the surface of a cyber attack (2016)

“...The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It’s about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation.”

Contacts

Marta Ganko  
National Privacy and Data Protection Lead, Risk Advisory  
Sydney  
+61 2 9322 3143  
mganko@deloitte.com.au

Greg Janky  
Partner, Risk Advisory  
Melbourne  
+61 3 9671 7758  
gjanky@deloitte.com.au

Puneet Kukreja  
Partner, Risk Advisory  
Melbourne  
+61 3 9671 8328  
pkukreja@deloitte.com.au

David Owen  
Partner, Risk Advisory  
Sydney  
+ 61 2 9322 7679  
dowen@deloitte.com.au

Tommy Viljoen  
Partner, Risk Advisory  
Sydney  
+61 2 9322 7713  
tfviljoen@deloitte.com.au