Board talk - Dealing with data privacy

Authors:

Paul Black
Partner
Forensic Risk, KPMG Audit, Assurance & Risk Consulting

Kelly Henney
National Leader
Privacy Services, KPMG Audit, Assurance & Risk Consulting

Data is fast becoming one of the most important intangible assets for organisations. Data sets organisations apart, enabling better product development, and personalised service offerings, making it a source of competitive edge.

However, the growing commoditisation of data and the advent of serious data breaches across jurisdictions and industries has called for sweeping regulatory change to codify accountability and transparency.

Regulations such as the Notifiable Data Breaches scheme (NDB scheme) and General Data Protection Regulation (GDPR) are lifting the standard on security measures, organisation-wide data awareness, and restoring trust and ownership of personal data with consumers. These regulations also seek to increase accountability for breaches. Fines are only the beginning of repercussions, with reputational damage having long-term downstream effects for consumer trust and bottom lines.

Boards are increasingly facing data related risks and issues. New regulation, and community expectations, need to be balanced with strategic objectives for digital transformation, reducing operational costs, and retaining competitiveness while delivering on the value proposition. Data lakes and organisation-wide practices need to be understood, and the controls for ethical use and protection of this data need to be monitored and communicated at all levels.

Some of the key data related issues facing boards today are governance, regulation, consumer trust, security, preparation and response, and data strategy and technology innovation.

Governance

Good governance has never been more critical. In an environment of sweeping regulatory change and heightened consumer awareness of data risks, conflicts often arise between data mining mandates, legal requirements and ethical consumer considerations. Asymmetrical dissemination of privacy risk appetite throughout the organisation, and disempowered risk governance across delegations of authority, usually result in revisiting decisions and potentially higher costs to rectify poor privacy compliance solutions.

Without clear guiding principles regarding how an organisation treats consumer data, there remains risk of grey areas. In relation to consumer data, good governance means:

- data principles that align with consumer expectations, board risk appetite, and organisation values
- enforcing, monitoring and reporting in relation to data governance and controls
- mechanisms for monitoring regulatory change
- clearly defined roles and responsibilities, with empowering delegations of authority
- managing conflicts with business uses of data, and secondary uses
- ensuring data principles are instilled throughout the organisation through regular training, enforcement and real consequences.

Without good governance, the framework for data management will not be clear, and there is likely to be less visibility of data practices, therefore leading to a higher likelihood of breaches.

Regulation

Since 22 February 2018, notification of eligible data breaches became mandatory in many cases to the Office of the Australian Information Commissioner and affected individuals through the NDB scheme. This is the first time in Australia that all entities that are covered under the Australian Privacy Principles have clear obligations to report on eligible data breaches. A critical part of being able to comply with the NDB scheme is preparation. Entities need to know what information they have, where it is stored, how it is protected, how they'll know when a data breach has occurred, and then how they'll respond.

Since 25 May 2018, the GDPR came into force with extraterritorial reach that has implications for Australian businesses that offer goods and services to individuals in the EU, and/or monitor EU individuals. This regulation introduced significant requirements for understanding organisation data processing activities (records of processing), providing significant data subject rights such as the right to be forgotten, and data breach reporting requirements of 72 hours from the point of awareness. Broadening the brush stroke of this regulation are the fines, which range from €20 million to 2-4% of annual global turnover or whichever is higher.

There is significant compliance burden, and risk of reputational and financial loss entailed in meeting these imposing obligations. In raising the bar for transparency and accountability for personal data managed by organisations, these regulations are also a source of many unknowns for non-EU organisations as the enforcement has yet to be tested by privacy regulators.

Upcoming regulation called the Consumer Data Right will start with Open Banking and ultimately be implemented across the entire market, with the energy and telecommunications industries next.

Consumer trust

The Australian Community Attitudes to Privacy Survey 2017 found that privacy awareness was growing, however the majority of respondents did not use, or did not know how to use, simple safeguards such as clearing cookies to protect their privacy

In 2018:

- Approximately 150 million customer accounts, including personal emails and passwords, were affected by the myfitnesspal breach of March 2018.
- Orbitz, a travel site owned by Expedia, also disclosed a breach that resulted in unauthorised access to 880,000 personal credit card details for customers who booked travel over 2016 and 2017.
- Cambridge Analytica used the data of 50 million Facebook customers without consent to build psychological profiles so voters could be targeted with ads and stories.

Such data breaches, and the approaches to resolution for affected individuals, indicate a shift in accountability and transparency.

The NDB scheme and GDPR most notably brought into effect mandated data breach investigation and reporting timeframes. These laws also increased accountability through introducing significant fines. Breaches also impact reputation due to public reporting.

However, regulation alone is not enough. Attitudes of organisations towards their customer's personal data and consumer expectations about the fair use of their data need to align. Customers expect organisations to fulfil service and product obligations, remain competitive and profitable, while also protecting their privacy interests.

One way organisations can achieve this is through transparency over internal and external data flows, communicated through clear, concise privacy statements. Giving consumers control over how their data is collected, and making the processes for setting such preferences easy and amenable to different customer groups, also need to be considered.

Underpinning this is how serious organisations are about data protection. Organisations must be assured that third party arrangements preserve customer privacy interests. Further, investments in sustainable technology solutions, and automation of manual processes can improve the efficacy of privacy management.

Security

Strategic objectives for technology transformation, use of social media engines and upgrading legacy systems increase exposure to the risk of cyber-attacks. With organisations becoming more interconnected and reliant on complex IT systems, exposure to cyber-attacks has become more sophisticated, frequent, targeted and difficult to detect. As a result, cyber-related crime is one of the highest rated risks facing organisations today.

New regulation seeks to instil requirements for having adequate safeguards that are commensurate with the scale/impact of threats to which an organisation is exposed. Organisations should also have active measures to protect personal information held, while also having measures to ensure data troves are not retained unnecessarily. These requirements are reflected in APP 11, Article 32 of the GDPR, and current draft APRA prudential standard CPS234 information security.

It is incumbent on organisations to take appropriate and proportionate technical and organisational measures to manage security risks. Organisations can achieve this by integrating preventative measures to safeguard privacy, raising awareness of every employee's role in data protection, and distributing responsibility across all levels of an organisation. To tackle the increasing threat of cyber security, common controls embedded throughout organisations include:

- pseudonymisation and encryption
- confidentiality, integrity, availability and resilience of processing systems
- restoring availability and access to personal data following a cyber-attack
- monitoring and supervision of technical and organisational measures.

Preparation and response

The ability to quickly detect, respond and recover from a cybersecurity event has never been more critical, with the volume of cyber-attacks at an all-time high, and the ever evolving local, and global legislative environment.

Cyber risk poses an asymmetric threat to governments and businesses alike. Hacktivists, insiders, criminals and nation states have a range of motives for stealing, disrupting or destroying information and the systems that they rely upon. Couple this with the increasing pace of technological development, and the growing dependence of organisations on digital information and interconnectivity, and you have a challenging business risk which requires a dynamic solution.

Investors, governments and regulators are increasingly challenging board members to demonstrate diligence in the area of cybersecurity. Regulators expect personal information to be protected, and systems to be resilient to both accidental and deliberate attacks.

One of the most common causes of a failed response is inadequate preparation, and many organisations suffer significant brand, reputational and financial impact as a result of poor planning processes, and disproportionate or inadequate incident response capabilities. It is critical that cyber risks are understood, clear and defined responsibilities exist, and response plans are current, practical, and most importantly, tested.

Restoring trust and minimising reputation damage is a significant challenge to organisations, and without a strategy that encompasses more than just security, the fallout from a breach is likely to be significant. The combination of people, privacy, information governance and business resilience is key to managing cyber risk.

Data strategy and tech innovation

As organisations seek to improve the customer experience and secure the competitive advantage associated with brand trust, it is crucial to leverage customers' personal information assets in the most appropriate way. Organisation strategies often lean on the analytics potential of big data to drive competitive positioning for operational efficiency and improved product offerings. However, this needs to be tempered with the risk of cyber and data breaches, and requirements for data minimisation.

Quality data is at the heart of a strong data strategy which includes automation and AI initiatives to replace and enhance existing business processes. However, large lakes of unstructured data can hinder the ability to access effective insights. Further, boards are concerned about the mismatch in maturity of organisation-wide data governance practices with the speed of automation deployment. This generally results in organisations taking on more risk than contemplated in project phases. This is where effective Privacy Impact Assessments (PIAs) are critical to ensuring personal data risks are detected and managed.

Further, automation and AI bring new risks, such as potential biases in those writing algorithms, ineffectiveness of existing controls to monitor performance of algorithms, and lack of suitability of existing risk frameworks to extend over analytics practices. Therefore, existing employees will need to invest in training to learn new skills as their roles evolve.

Looking forward

We have explored some key risks facing boards today. As the pace of automation, investment in new technologies, and machine learning accelerates, new regulations and community expectations will need to be navigated to ensure personal data is adequately protected.

However, new regulation and the fear of customer expectations should not be a hindrance to evolving business practices, being courageous in exploring analytics, and designing tailored products for consumers that offer price, choice and flexibility. While consumer awareness of data privacy is currently at its highest measured levels, organisations need to finely balance these heightened expectations with meeting efficiency and competiveness objectives. Organisations should not be afraid to use the data they have, as long as they have confidence that it is well protected, backed by lawful processing and anonymised or pseudonymised where appropriate.

Building consumer trust by enforcing strong policies around data governance, protection and consumer control will be the difference between organisations that thrive and those that fall behind.

For further information, view the videos here.