Digital Trust: The Key to Unlocking the Promise of a Digital Economy
Trust is the cornerstone of the digital economy. Without it, Australian businesses cannot use and share the data that underpins their operations.
Customer trust in Australian businesses will be tested under proposed data breach notification laws. To avoid damage to their reputation, businesses must have strong security and digital ethics at each stage of the customer journey. Those that get this right will enjoy a competitive advantage as we usher in the digital future.

In 2014–15, the Australian Cyber Security Centre responded to 11,773 cyber security incidents affecting Australian businesses. Of these incidents, 218 involved systems of national interest and critical infrastructure. Only recently, the Australian Bureau of Meteorology was the victim of a high-profile cyber intrusion.

This is a wake-up call for Australian businesses and enterprises; and attacks, including more sophisticated ones, are only going to increase over the next three to five years. The threats are real, and those that fail to take them into account are not only letting their customers down, they are exposing their businesses to financial and reputational risk.

“Security breaches can damage not only the reputation of companies that are breached, but also the reputations and material interests of their customers,” Irvine says. “This increases pressure on Australian businesses. Legally, they must comply with privacy laws; ethically, they are responsible for protecting their customers’ data; and commercially, they are under pressure to limit the risk of breaches damaging their operations and reputations.

“Companies that succeed in these areas will attract customers looking for service providers they can trust to protect their data.”

There is little doubt cyber security is on the national agenda, with the Australian Government announcing a $230 million Cyber Security Strategy, including plans for a Cyber Security Growth Centre. This is particularly timely as cyber adversaries become increasingly sophisticated, making detection more difficult.

---

86% of Australian executives agree that trust is the cornerstone of the digital economy.
After the consumer outcry over its iCloud breach in 2014, Apple came to understand afresh the importance of trust. Its efforts to be transparent in how it uses and secures customer data is testimony to the value this leading brand places on trust. Its new platforms, such as Apple Pay and HealthKit, are clear beneficiaries of a trusted-by-design approach in which strong security and ethics are 'baked in', giving customers confidence that their digital footprint is secure and private, and easing the transition to the Apple ecosystem. This underscores the role trust plays as digitally powered companies look to disrupt their own markets and enter new ones.

Companies that understand the vital role trust plays in the digital economy know that in order to compete, push boundaries and offer new services, they must design products and services that are both ethical and secure by design. For example, Microsoft is opening data centres in Germany that will be managed and operated by a third party, allowing German customers to use Microsoft technology but to have all their data controlled by a German company, without being accessible to Microsoft.

"It is vitally important for service providers, and other custodians of customer personal or commercial data, to protect that data against criminal or other unethical or improper exploitative activities that could be prejudicial to the right to privacy, the personal reputation or commercial interests of the individual subject of the data. The recent Panama Papers incident is an example of this. Many of Mossack Fonseca’s customers have not been proven to have broken any laws or illegally evaded any taxes, but their reputations have been thrown into doubt by the failure of the custodian to protect customer data entrusted to it."

David Irvine AO, Chair of the Australian Cyber Security Research Institute and former Director-General of Security in charge of ASIO.
By building new offerings in this way, Australian companies can create trust and minimise systemic risk. This is critical – especially where data is needed to inform personalised services at scale, using technologies that require troves of personally identifiable information. As the business value of data grows, 85 per cent of Australian executives agree or strongly agree that the risks companies face from improper handling or disclosure of data are growing exponentially. Managing that risk and building trust starts with data ethics and security.

Recognition of new risks from digital transformation has already propelled security investments across all industries. Spending on information security is growing rapidly in Australia, but even so, a singular focus on security is insufficient to account for the risks encountered by digital businesses.

More than 86 per cent of Australian companies are required to comply with data handling protocols that go beyond their internal controls. To account for these intrinsic risks in other parts of a business’s operations, data ethics and digital ethics are critical.

Although consideration of ethics should be a key part of digital transformation, it’s a new area of focus for the majority of businesses. It’s not just customers who are sounding the alarm – 87 per cent of Australian executives say their knowledge workers are demanding stronger ethical controls on data too. Currently, most companies’ strategies align to a single factor: privacy – which is just one component of data ethics. Digital ethics is even broader, and includes any instances where data is used to affect business outcomes, strategies, programs or campaigns.

Data Ethics vs Digital Ethics

**Data Ethics**

“What are my ethical obligations to protect this data from wrongful disclosure?”

**Definition**

Moral governance of the integrity, handling, control and provenance of data.

**Digital Ethics**

“Can I use this customer data for a purpose different to that which the customer initially consented?”

**Definition**

Data ethics and moral governance of actions taken as a result of insights derived from the analysis of information (where ‘information’ is data with context).
Company boards, and their risk committees in particular, need to pay attention. Without comprehensive policies, training, incentives and consequences for transgressions of data and digital ethics, exposure to risk increases and adverse outcomes are more likely. Board and risk committee members have a critical strategic role in promoting diligence around digital trust, and focusing on cyber security across the business. This is important to ensure a solid framework of governance, minimising business exposure to negligence on the part of an individual.

One way to account for this risk is to consider whether trust is being enhanced or eroded at every step of the customer journey. What's more, if companies fail to recognise and 'design in' strong ethical controls that account for cultural variances in governance, and human and technological processes throughout the customer journey, they face further damaging outcomes. Eighty-six per cent of Australian

survey respondents agree that companies lacking security, privacy and ethical controls on data risk exclusion from future data ecosystems – an increasingly important aspect of go-to-market strategies.

Businesses will start adopting 'hunting' techniques and platforms that proactively seek out cyber adversaries from within their business environment. This approach further supports the ability to defend and secure an environment to ensure confidentiality, integrity and authenticity of data within the business ecosystem. Going from reactive to proactive defence will become the new business norm to ensure trust with business stakeholders.

86% of Australian executives agree that companies lacking security, privacy and ethical controls on data risk exclusion from future data ecosystems.

New Responsibilities
Australian businesses must identify an executive responsible for developing governance models, taxonomies and principles-based codes. This role will also focus on technically challenging areas such as decision making in autonomous systems, and confront today’s assumed definitions of informed consent and what it means to be truly anonymous. These are no longer philosophical puzzles. They are critical business realities that all companies must solve.

1100
1010101010101010101010101010101010101010000010101111110000101010101010
110010101010101010101010101010101010101010000010101111110000101010101010
110010101010101010101010101010101010101010000010101111110000101010101010
110010101010101010101010101010101010101010000010101111110000101010101010
110010101010101010101010101010101010101010000010101111110000101010101010

In addition, a failure by companies to address data and digital ethics may prompt regulators to impose their own rules and legal frameworks. Any change in the regulatory environment can force changes to business models. Look at how the 2015 invalidation of ‘safe harbour’ by the European Court of Justice caused scores of companies to redesign how they share personally identifiable information between the European Union and the US.

Wherever regulatory scrutiny strikes next, one thing is certain – corporate indifference to data and digital ethics can increase risk to a company’s reputation and create unwelcome headlines. In order to deliver against their responsibilities, company boards and CEOs must focus on implementing the right systems and processes to mitigate this risk.

Locally in Australia, shopping site Catch of the Day was heavily criticised after it revealed that encrypted passwords and user information had been taken from its database three years earlier.

---

Trust and the Customer Journey

**Role of Trust:**

- **Differentiation**
  - Transparency of ethics and security practices can set your brand apart from others.

- **High Ethical Standards**
  - Adhering to high ethical and security standards may require similar updates on connected platforms.

- **Trust Attracts Customers**
  - As products and services become more trustworthy, customers become advocates.

- **Maintain Strong Relationships**
  - Customers become partners and build on top of your platforms; you have more leeway to experiment.

**Customer Journey:**

- **Consider**
- **Purchase**
- **Integrate**
- **Maintain**
- **Advocate**
Making the right decisions internally to gain customer trust is only half the battle. Making sure that neither outsiders nor ‘trusted’ insiders gain unauthorised access to data and abuse hard-won trust is also crucial. That’s why next-generation security mechanisms are following the data, taking user behaviours into account and extending well beyond the perimeter. Wherever data goes, security must go with it. To address this challenge, security solutions – such as security-aware application design, integrated database security, dynamic access controls and runtime application protection – are being integrated into new products. Security orchestration across an entire business ecosystem will become essential to proactively identify and respond to real-time threats within the environment, and to maintain digital trust.

This data-centric philosophy is also revolutionising identity and access management. For example, InAuth, a mobile-device security company, establishes the trustworthiness of a device before granting it access to network resources. Once a device is validated, solutions from the likes of BioCatch employ multifactor authentication, which considers the way users interact with devices, as a way to verify and provide persistent identity.

A number of organisations are also exploring how blockchain, a public ledger of bitcoin transactions, could provide a way to industrialise and automate trust. Not only does this provide an alternative to the current organisational and procedural methods, it would fundamentally transform how they achieve trust.

Global companies are also moving decisively in this direction. For example, AT&T is undertaking a wholesale upgrade of its back-end architecture, moving toward data-centric security in its databases and applications. It’s doing this to ensure high data integrity, so data is stored securely and not manipulated in transit. Coca-Cola, Verizon, Google and Mazda are all taking a similar approach. Embracing this transformation, their leaders understand that trust comes from robust security and data ethics.

The scalability enabled through the digital transformation of the customer journey has positive and negative dimensions. The best way to minimise downside risks is to maximise trust. Better security on its own won’t be enough; nor will rote compliance with privacy regulations. Australian organisations must manage data and digital ethics as core strategies for mitigating business risks, just as they do with cyber security. Their reward? Unprecedented growth in an interconnected platform economy, with significantly reduced downside risks. Those who master this transformation can move beyond the first level of customer trust—namely, that products will meet or exceed expectations—to a higher level where individuals trust a company to lead them into the digital future.
Predictions

Looking to the future, displaying trust and digital ethics will continue to play an increasingly critical role in Australian business operations and become the minimum standard for participating in industry ecosystems.

The Trust Bust: High-profile digital ethics failures will create new governing bodies in Australia, new regulations and a new category of jobs.

The CEO Gets a Twin: Trust becomes paramount, and a new leader emerges – the Chief Ethics Officer.

Key Takeaways

- Ethics and security must be primary considerations in any digital transformation. Digital trust will be as important as security if companies are to continue to do business.

- Customers will increasingly turn to companies they can trust to protect their data.

- Exposure to risk scales in proportion to digital business operations.

- Australian businesses could risk financial penalties and damage to their reputation under data breach notification laws proposed in Australia.

- To protect against downside risk, businesses must foster strong ethical decisions, effectively use security to protect against external threats, and build trusting relationships with ecosystem stakeholders.

- In procuring new technologies, security and ethics must be key evaluation criteria.

- Businesses must look for opportunities to build trust at every engagement point along the customer journey.
Digital Trust: 100-Day Plan

Over the next three months, businesses should work to understand the current state of digital risk they're exposed to and benchmark data points that can be improved.

1. Survey stakeholders to quantify the level of trust across your product portfolio.

2. Search customer service logs for the word 'trust', and run sentiment analysis against the results to gain an understanding of how customers perceive your offerings and brand; make a top-five list of the least trustworthy offerings.

3. Take an inventory of data-driven business processes; describe the current and potential opportunities for enhanced security and data ethics for each, including preparedness for Australia’s proposed mandatory data breach notification laws.

4. Identify the executive(s) responsible for building and maintaining trust; digital ethics; security; and compliance with vendors, partners, customers and regulators.

5. Research what your competitors and other leading organisations do to build customer trust. Record what builds and erodes trust. Brainstorm opportunities for improvement within your own operations.

6. Consider partnering with an academic institution, non-profit or industry group to dive deeper into one aspect of digital ethics or security. The innovative solutions that can result from such a partnership have the potential to markedly increase a company’s security posture.

7. Compile a list of opportunities for security to move closer to the data used by the business, and investigate ways that data can be secured.
1. From the top-five list of the least trustworthy products, do a complete customer journey analysis and try to understand where opportunities exist to build trust.

2. Discuss hiring a chief digital officer, chief trust officer or chief ethics officer with your board of directors. This role will be responsible for orchestrating the establishment and maintenance of digital trust.

3. Pick one product or service to maximise trust. Build metrics for tracking improvement over time, including metrics for regulatory compliance and responsiveness to data security breaches. Report results to product teams and challenge them to meet targets.

4. Start tracking metrics for trust, and data and digital ethics, including metrics for regulatory compliance and responsiveness to data security breaches. Use this data to include trust and ethical practices in your company’s annual corporate social responsibility report.

5. Implement a portfolio of solutions to move security closer to data. Describe how their implementation has mitigated downside risk. Share this report with your CIO and CFO in an effort to reduce insurance premiums.

Within a year, businesses should have started to include provisions for strong digital ethics in their digital transformation strategies, have new pilots underway, and have concrete plans to mitigate violations of customer trust and respond to breaches.
About Us

About Accenture Technology R&D

Technology Vision is published each year by Accenture Technology R&D, the dedicated research and development organisation within Accenture that includes the Technology Vision group, Accenture Open Innovation and Accenture Technology Labs.

For more than 20 years, Accenture Technology R&D has helped Accenture and its clients convert technology innovation into business results. Our R&D group explores new and emerging technologies to create a vision of how technology will shape the future and shape the next wave of cutting-edge business solutions.

We offer seminars on the Technology Vision, which provide a forum to discuss the trends in greater depth and explore the implications for your organisation.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 375,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

For more information, please contact:

Jean-Marie Abi-Ghanem
Accenture Security Practice Lead, APAC
j.abi-ghanem@accenture.com

#techvision2016

The views and opinions expressed in this document are meant to stimulate thought and discussion. As each business has unique requirements and objectives, these ideas should not be viewed as professional advice with respect to your business.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.