Deloitte.

The Deloitte Consumer Review

Risky business: Keeping up with the changing consumer

September 2018

Contents

About this report
In this publication, references to Deloitte are references to Deloitte LLP, the UK affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited.

Methodology
The research featured in this report is based on a consumer survey of 2 001 UK adults carried out by an independent market research agency on behalf of Deloitte.

Please visit http://www.deloitte.com/view/consumerreview for additional content related to the Consumer & Industrial Products industry.

Executive summary

Consumers and businesses are adopting digital technology at a rapid pace, and while this is generating new opportunities, it is also creating new risks.

Consumers have been empowered by digital technology and the real-time access to price and product information that it brings. They expect personalised products and services, and want to engage with brands across multiple channels in a seamless way. They also expect companies to be transparent about the data they hold on them, what they use it for and how it is protected. A number of high profile cyber-attacks and the introduction of the General Data Protection Regulation (GDPR) have heightened consumer awareness of the risks of sharing their data with businesses.

The digital transformation of many consumer businesses is well underway and is impacting both the front and back offices. A heavy burden is being placed not only on the IT department but also on the internal risk function. Business leaders are making strategic choices on the investment, technology, resourcing levels and the skills needed to operate a digital business, all of which will have an impact on the short-term profitably and long-term viability of their businesses. These strategic choices inevitably involve an element of risk.

At the same time businesses have to cope with external threats. For example, as businesses undergo digital transformation and more of their assets become digital, the threat of cybercrime and risks around data privacy are growing. A recent Deloitte survey showed that 92 per cent of executives believe that cyber-security would have an impact on their organisation.

Research conducted for this report revealed that 68 per cent of consumers will be more careful about how they share data following the introduction of GDPR, while over half agreed that they would boycott companies that breached GDPR rules.

While the rate of digital adoption will be different for each organisation, we believe there are three areas that all businesses need to focus on as part of their digital risk management strategy:

- **Managing risk in a digital organisation** – Consumer businesses need to adopt a flexible and consistent approach to identifying and managing risks posed by new digital technologies, such as AI and machine learning, and new ways of working such as Agile and DevOps.

- **Managing risk digitally** – Governance, risk, compliance and control stakeholders should embrace digital technologies to optimise efficiency and predict risk and to generate insight on the 'controls environment'.

- **Managing digital transformation risk** – Businesses need to understand the risks of transformation to ensure they meet their objectives, while utilising the most appropriate technologies and deployment methodologies.

Digital disruption

Digital technology is not only disrupting the consumers' path to purchase, but also how businesses operate and manage risk.

The state of the digital nation

Empowered by technology that allows them to connect and share information with anyone, anywhere in the world, at any time, today's digital consumer expects a business to react to all their needs and wants instantly.

With the advent first of the home computer, followed by the laptop and in the last ten years the smartphone, the balance of power has shifted progressively away from business and towards the consumer. In the next ten years, we could see the rate of change accelerate as consumers make use of a new wave of innovative technology that could further tip the balance of power in their favour.

Digital technology has had a significant impact on our everyday lives. It influences how we work, our health and wellbeing, how we shop, and in the last decade, it has even begun to change the way we socialise. This process is set to accelerate as the first generation that grew up with the internet at their fingertips enters the world of work. We are already seeing the application of new technologies, including robots, the internet of things (IoT), artificial intelligence (AI), cloud computing, predictive analytics and blockchain rapidly changing the way many companies design and curate experiences, manufacture, distribute and service products.

As a society we are becoming more and more reliant on technology to complete everyday tasks. For example, technology is the driving force behind the move towards a cashless society, with over 85 per cent of consumers now using credit or debit cards regularly to pay for goods and services compared to 72 per cent in 2015. Although credit and debit cards have been in existence since the 1960s, this move towards a cashless society has gained momentum over the last three years as contactless technology payments have grown in popularity. The shift to a cashless society could also be expedited by the adoption of other technology. Our research shows that while 11 per cent of consumers regularly use digital wallets hosted on their mobile phones to pay for goods and services, this figure rises to 19 per cent of 18-to 24-year-olds and 21 per cent of 25-to 34-year-olds. Given the penetration of smartphones across the UK, and the higher propensity of younger consumers to use them for shopping and payments, this is expected to rise significantly over the next five years.

Digital business brings digital risks

Similarly in the world of work, businesses are increasingly reliant on digital technology. Networks and supply chains depend on connected technology, factories are becoming increasingly automated and many office workers already rely on their laptops and mobiles to complete standard tasks.

The increasing reliance of both consumers and businesses on technology is also exposing them to new and changing risks, many of which are not fully understood. What is perhaps more worrying is that a number of businesses do not have the right governance, processes and controls in place to safeguard their consumers, their employees and their brand.

An escalating risk

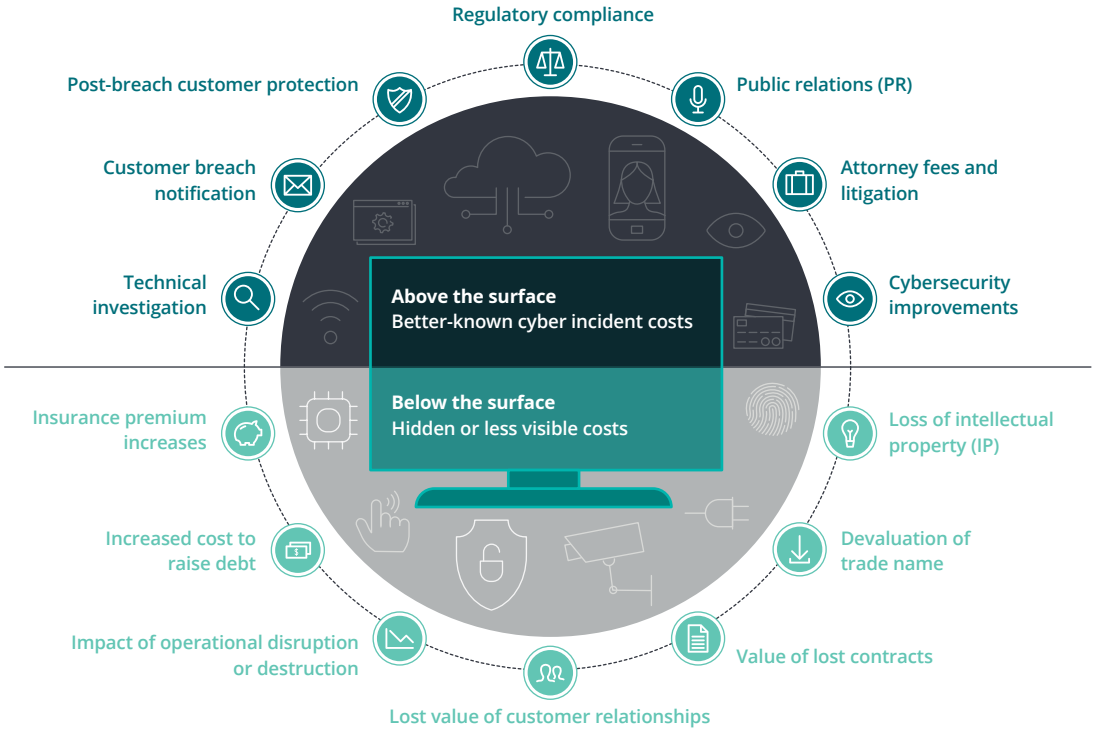
Cybercrime is on the rise, not only in the number of attacks but also in their severity. Many organisations are still unprepared to deal with different types of attacks and are at best aiming to mitigate the risk, rather than preventing attacks in the first instance.

Businesses are collecting more data and are also becoming increasingly dependent on it for their day-to-day operations. In a world where cybercrime is becoming ever more lucrative, businesses are exposed to more security risks than ever before. As more of their assets become digital, the risks and implications of cyber-attacks are intensifying. Therefore, businesses in the consumer sector need to have a strategy in place to deal with such attacks.

"Digital technology has had a significant impact on our everyday lives. It influences how we work, our health and wellbeing, how we shop, and in the last decade, it has even begun to change the way we socialise."

Figure 1: 14 cyber attack impact factors

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident.



Source: Deloitte University Press[1]

This report looks at three areas where our increasing dependence on digital technology is exposing both consumers and businesses to risk. The three areas are:

1. Digital transformation
2. Cyber-security
3. Privacy and data protection

The following sections examine the consumer and business dimensions of each of these areas, the risks they present and then in the final section of the report we explore the steps businesses should take to address them.

Digital transformation: Risk and reward

While digital transformation is creating major opportunities for consumer businesses, it is also introducing a new dimension to the traditional view of risk.

Driving the digital transformation of business is an unprecedented level of investment in digital technology, innovation, and research and development. According to a recent Deloitte survey of 106 executives responsible for digital technologies in some of the UK's most influential companies and public sector bodies, 36 per cent of organisations have already invested over £10 million in digital technology, with another 49 per cent planning to invest that amount by 2020[2].

However, this level of investment also gives rise to a number of risks. Any business involved in transforming their digital capabilities through high levels of investment will need to think carefully about the impact such change will have on their overall strategy, culture and people.

Many business leaders do not see their businesses and the talent within their organisations as being ready to cope with these changes including the role AI will play in arbitrating decisions on behalf of consumers. Indeed, our survey found that 65 per cent of organisations do

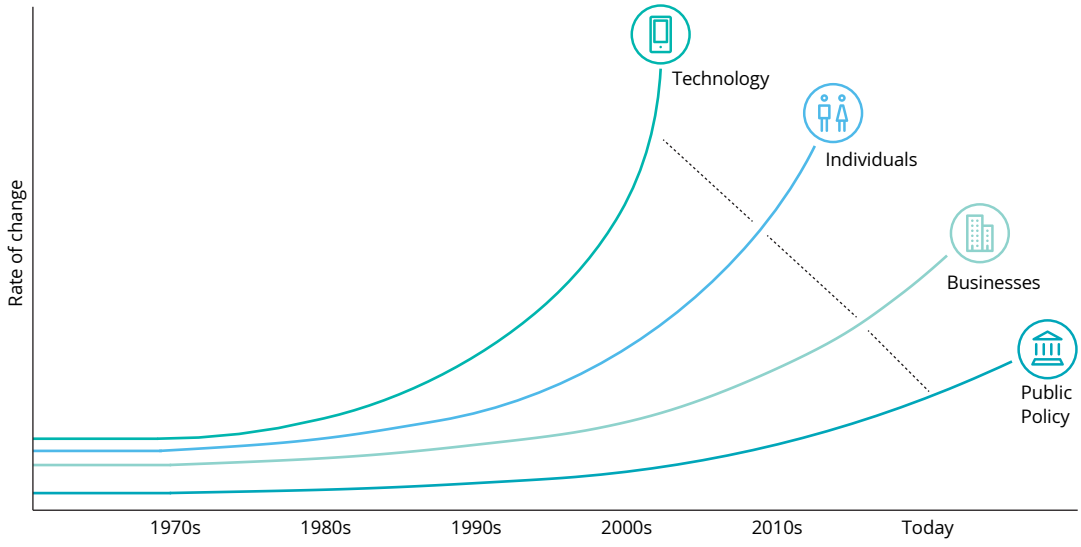
not believe their current talent pool has the sufficient knowledge and capabilities to execute and realise the full benefits of their digital strategy.

Moreover, 87 per cent of organisations believe they will need to change the way they engage with their workforce as they adopt new digital technologies and ways of working. Three-quarters of organisations surveyed agreed that it is difficult to attract and recruit people with the appropriate digital skills and experience, while 64 per cent agreed that their organisation finds it difficult to retain those people with the appropriate skills and experience.

Keeping up with the consumer

Technology is evolving at a faster rate than businesses can manage, shortening product lifecycles and challenging investment cycles and IT 'roadmaps'. At the same time businesses are struggling to keep up with consumers as they increasingly adopt the latest digital technology. Perhaps most worrying is that governments and regulators have been the slowest to react, exposing both businesses and consumers to potential risks.

Figure 2: Relationship between the rate of technology adoption among individuals and businesses



Source: Deloitte Human Capital Trends 2017

Understanding the risks of transformation

Digital technology has helped more businesses to connect directly with their consumers by creating new platforms for engaging with them or by creating new channels to sell to them. Digital technology has also created new ways for consumers to shop for products and services and to engage with brands. It has allowed both established players and start-ups to develop new business models to cater to this changing consumer behaviour.

Digital transformation can improve the efficiency of operations and ultimately reduce costs. Adopting new technologies often requires changing both the way that people work and the culture of an organisation. However, new technologies can also introduce new risks and the challenge for many businesses is how to identify, evaluate and mitigate such risks?

Cybercrime: A known but growing risk

As digital transformation continues, and consumers become dependent on technology, the potential for cybercrime has grown dramatically.

Not if, but when

From a business perspective, cybercrime has become so prevalent that it is a question of when, not if, your business suffers an attack. According to a recent Deloitte survey, 46 per cent of businesses have had to mobilise their crisis management teams to deal with a cyber-incident over the past two years. Indeed, the Deloitte Crisis Management Survey identifies cyber-incidents as a more serious threat to businesses than safety incidents, security incidents, performance issues, or government and environmental incidents[3].

With the potential for cybercrime growing it is no surprise that business leaders are focusing on the threat it poses to their organisation. In a recent Deloitte survey, 92 per cent of executives indicated that cyber-security would have an impact on their organisation and 67 per cent reported that it would have a significant impact. Four-fifths said their organisation had already invested in cyber-security, while an additional 9 per cent expected to invest by the end of 2018[4].

Consumer concerns on cybercrime are rising

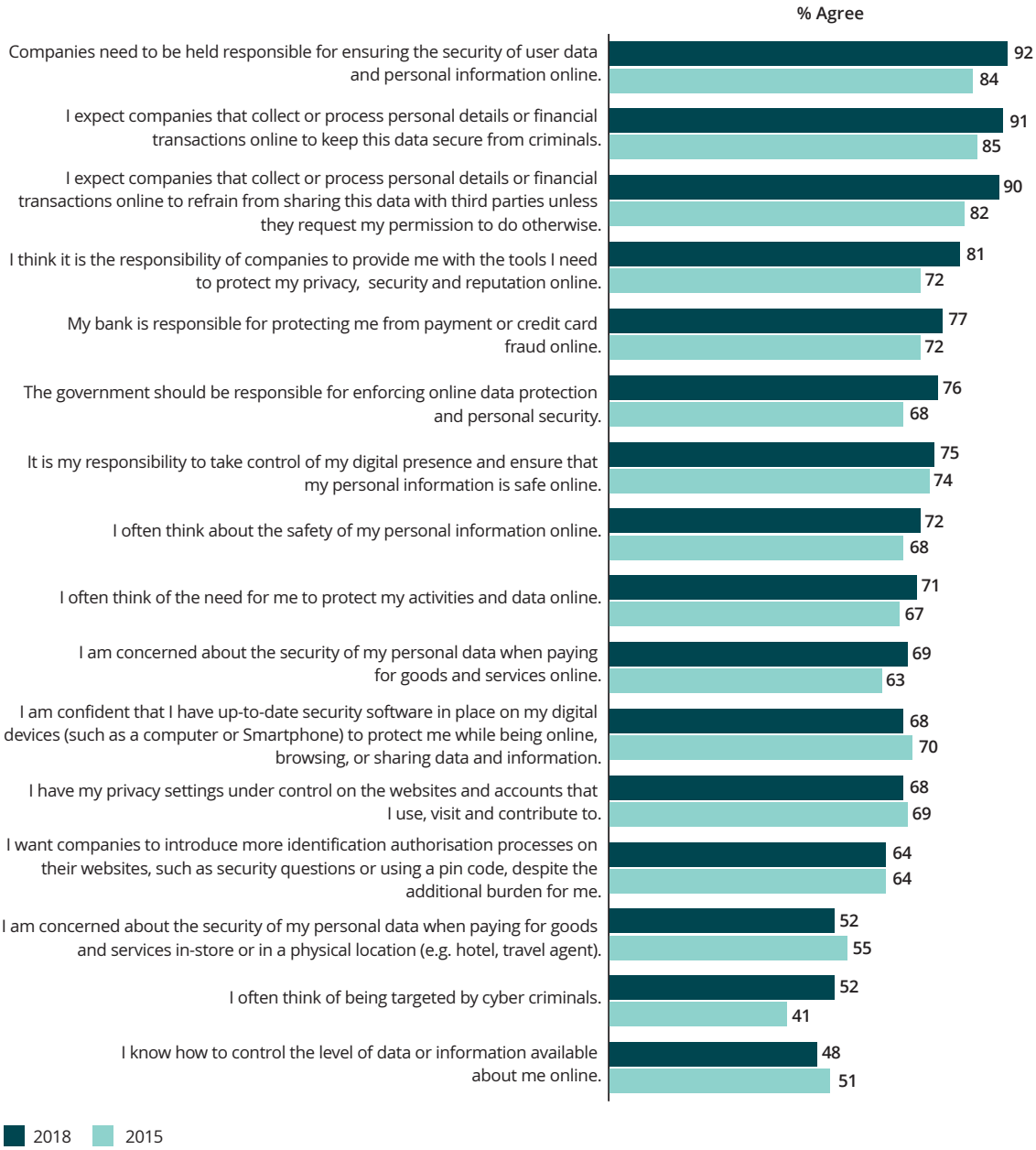
There is a real imperative for businesses to guard against cybercrime because there is a growing belief among consumers that organisations should not just be responsible for providing security, but should also be accountable for the impact of cybercrime. Deloitte research shows that 92 per cent of consumers believe that businesses should be held responsible for ensuring the security of user data and personal information online. Even when consumers acknowledge their own responsibility they still say that businesses need to play a role in facilitating their safety online with 81 per cent expecting companies with whom they share their data to provide them with the necessary tools to protect that data online. Consumer businesses therefore should ensure that they invest to strengthen their own defenses and to help consumers protect themselves.

This investment may include measures to prevent unauthorised access to data (e.g. personal or payment card data), improve the cyber security of an organisation's supply chain, raise the level of employee training and awareness, and develop a strategic roadmap to enable the organisation to stay ahead of emerging security threats. Attacks cannot be avoided, but investment in preventative measures will help to reassure consumers that the security of their data is important to your organisation.

"Deloitte research shows that 92 per cent of consumers believe that businesses should be held responsible for ensuring the security of user data and personal information online."

Figure 3: Consumers' attitudes to data security and cybercrime

Now thinking about the security of your personal data, to what extent do you agree or disagree with the following statements?



Source: Deloitte

Developing the appropriate response

The goal of a coordinated strategy should not only be to protect your business from incoming cyber-attacks, but also to insulate your business and its customers from the impact of any attack that does succeed. Therefore businesses should – at the minimum – consider taking the following action:

1. **Develop an integrated approach to cyber-security with board-level accountability** – Boards are becoming more aware of cyber-risk as an issue but many have yet to realise the potential impact on their own organisation and strategy. Nor do they understand how to manage this risk in line with their risk appetite and UK Corporate Governance Code reporting requirements. The implementation of integrated cyber-risk governance procedures will ensure that the board is better informed of the potential impact of a cyber-attack and has direct oversight of risk management processes and budgets to mitigate such risk.

2. **Know your cyber assets** – Consumer businesses need to focus on their data assets and critical IT processes to understand where they are located, the controls that are in place and the risks associated in protecting their brand. The challenge is similar to protecting tangible assets: a business cannot protect what it does not know about.

3. **Develop a response plan** – Businesses in the consumer sector all need to be able to prevent cyber-security incidents. Therefore organisations need to have the capabilities in place to detect and respond to an incident in a controlled and planned manner.

In 2018 there have been numerous examples of security breaches significantly damaging a business. Response and recovery are key to reducing the impact of the breach on the organisation. Organisations that have a response and communication plan in place, and are proactive in engaging affected customers, have seen less of an impact.

"In 2018 there have been numerous examples of security breaches significantly damaging a business. Response and recovery are key to reducing the impact of the breach on the organisation."

Privacy: The value and vulnerability of consumer data

One of the key considerations when it comes to digital transformation, is the value and vulnerability of consumer data.

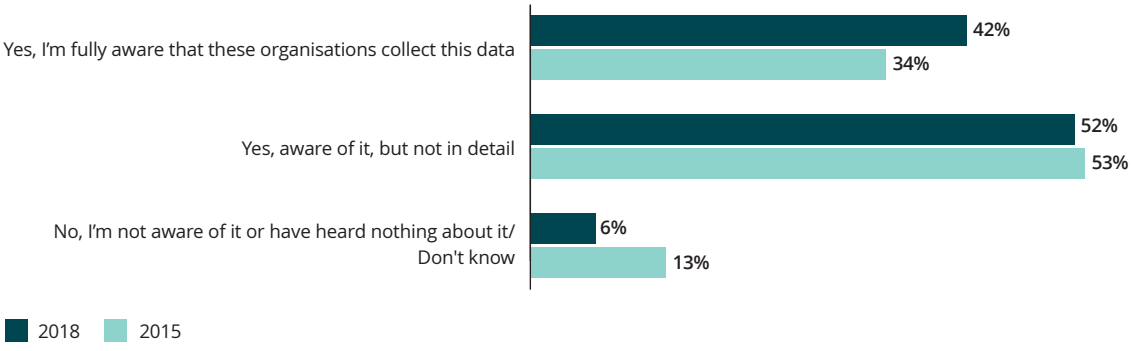
Our data footprints are getting bigger

With the greater use of digital technology, social media platforms and the increasing volume of online shopping, consumers' data footprints are increasing in size. How this data is collected, stored, used and shared by businesses has come under increasing scrutiny as consumers begin to realise the value of the data they have been sharing with organisations.

Consumer awareness of this issue has grown significantly over the last few years and reached a peak in 2018 with the EU's introduction of the General Data Protection Regulation (GDPR). More than 90 per cent of consumers are now aware of the extent that private and public sector bodies collect data about them and their activities.

Figure 4: Consumer awareness of data collection

To what extent are you aware or not that companies and public sector bodies collect data about you and your activities?



Source: Deloitte

Will GDPR have a long-term effect on consumer behaviour?

People now have greater control than ever before over their personal data following the introduction of the Global Data Protection Regulation (GDPR) on 25 May 2018.

GDPR marks the biggest change in data privacy legislation in over 20 years, and its introduction has shone a light on how businesses capture, store and use data. It has also prompted many consumers to reassess their attitudes to sharing their data with businesses. Our research found that when asked about the impact of GDPR, 59 per cent of consumers said that it has made them more aware of the data they share with business, while 68 per cent will be more careful about who they share their data with in the future. More than half (57 per cent) indicated that they would boycott companies that breached GDPR rules, and 41 per cent said they were happy to continue sharing their data.

GDPR Explained

Consent – where organisations need to get consumer consent, the bar has been raised to make this more explicit, although another lawful basis can be used if consent is difficult to obtain.

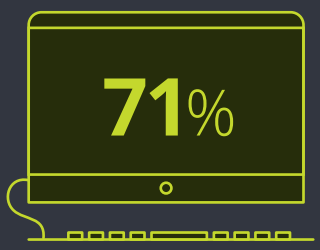
Breach notification – companies will need to notify consumers affected without undue delay when their data has been breached.

Right to be forgotten – consumers have the right to ask companies to erase their personal data. However, this right is not absolute and only applies in certain circumstances.

Data portability – consumers will have the right to ask to access the data companies hold about them and will have the right to pass on that data to other organisations should they wish to do so[5].

Digital Consumer Behaviour

I often buy goods from an online retailer

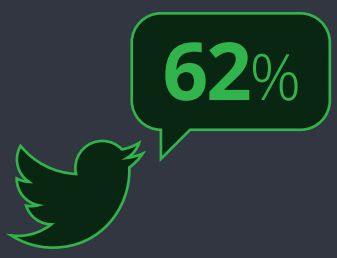


18–24s	25–34s
68%	75%

I often buy my groceries online

18–24s	25–34s
28%	36%

I often use social network sites



18–24s	25–34s
75%	77%

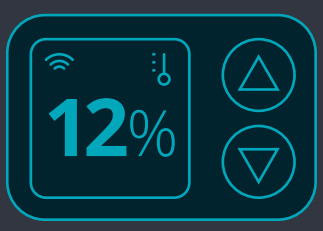
I often use messaging apps

18–24s	25–34s
79%	75%

I have access to at least one digital media subscription service

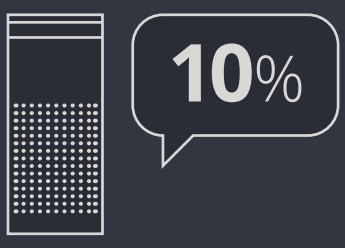
18–24s	25–34s
64%	57%

I have at least one internet connected smart device installed in my home



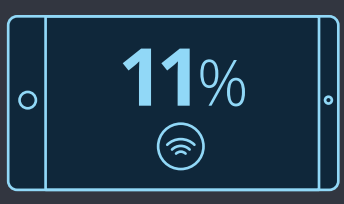
18–24s	25–34s
7%	14%

I own and use a voice controlled device at home



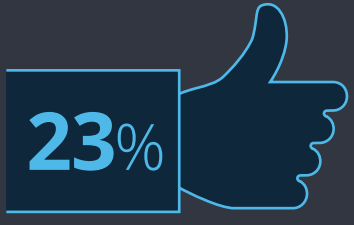
18–24s	25–34s
9%	9%

I often pay for goods or services using mobile solutions



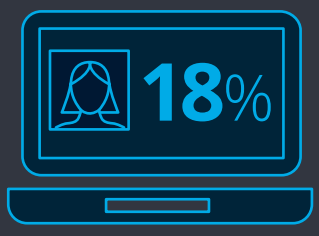
18–24s	25–34s
19%	21%

I often 'like', connect with or follow a company or brand on social networks



18–24s	25–34s
38%	37%

I often log-in to other web services using my social media profile



18–24s	25–34s
43%	30%

Source: Deloitte

Consumers are becoming increasingly conscious of the need to safeguard their own data in order to protect their privacy and reduce the risk of identity theft, fraud and the misuse of their data. From a business perspective, securing data and using it ethically is now vital as a breach of the new regulations could lead to substantial fines as well as negative headlines, damage to the brand and the loss of business.

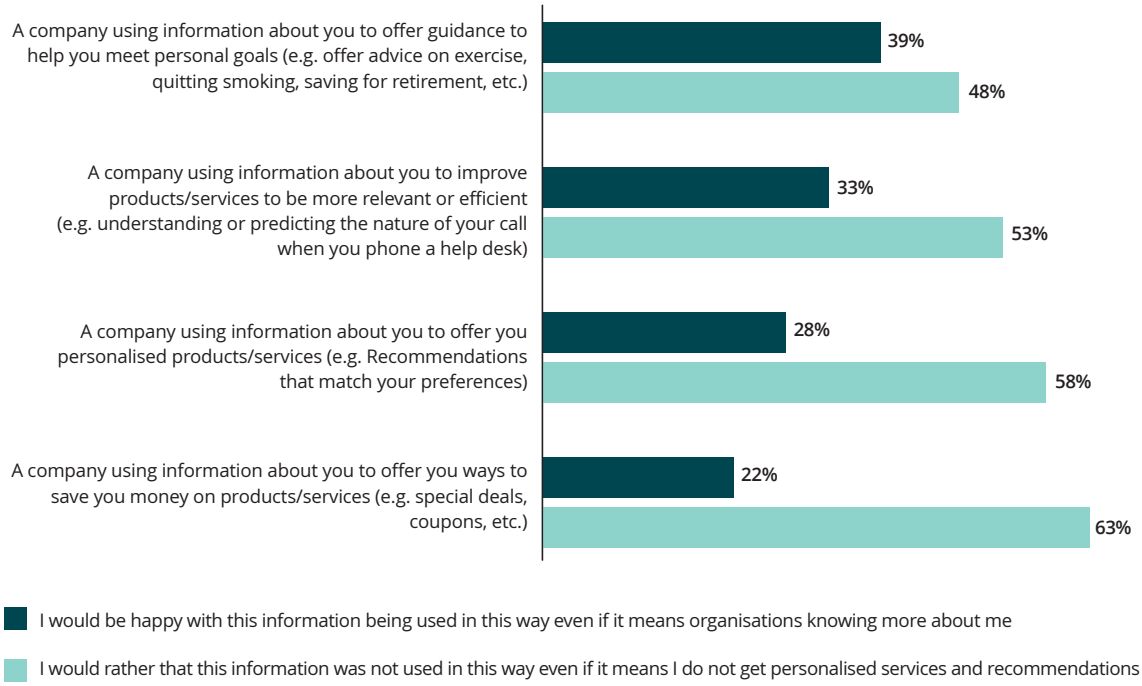
Justifiable concerns

As a result of GDPR, consumers are reconsidering their attitudes towards data sharing as well as the businesses with whom they are prepared to share their data. The concept of a value exchange where consumers are happy to share their data on the understanding that by doing so they get more personalised products, services or promotions is being challenged.

Deloitte's research shows the extent to which consumers are turning against the traditional value exchange. For example, despite being one of the key marketing tools for retailers, 63 per cent of consumers indicated that they are actually uncomfortable with businesses using personal data to offer money saving deals and coupons. Nearly 60 per cent said they would prefer that data not be used to offer personalised recommendations based on their preferences and past behaviour. This is worrying, especially for businesses that have sought to differentiate themselves based on the level of personalisation they are able to offer.

Figure 5: Consumer attitudes to data sharing

We are now going to show you some different scenarios about how personal information (contact details, date of birth, gender, marital status, purchase history etc.) can be used by organisations and companies (internet retailers, airlines, good manufacturers, banks etc.) in different ways. People are facing these scenarios in their day-to-day lives, or may face them in the future. For each of these, please indicate which of these two statements comes closest to your own opinion.



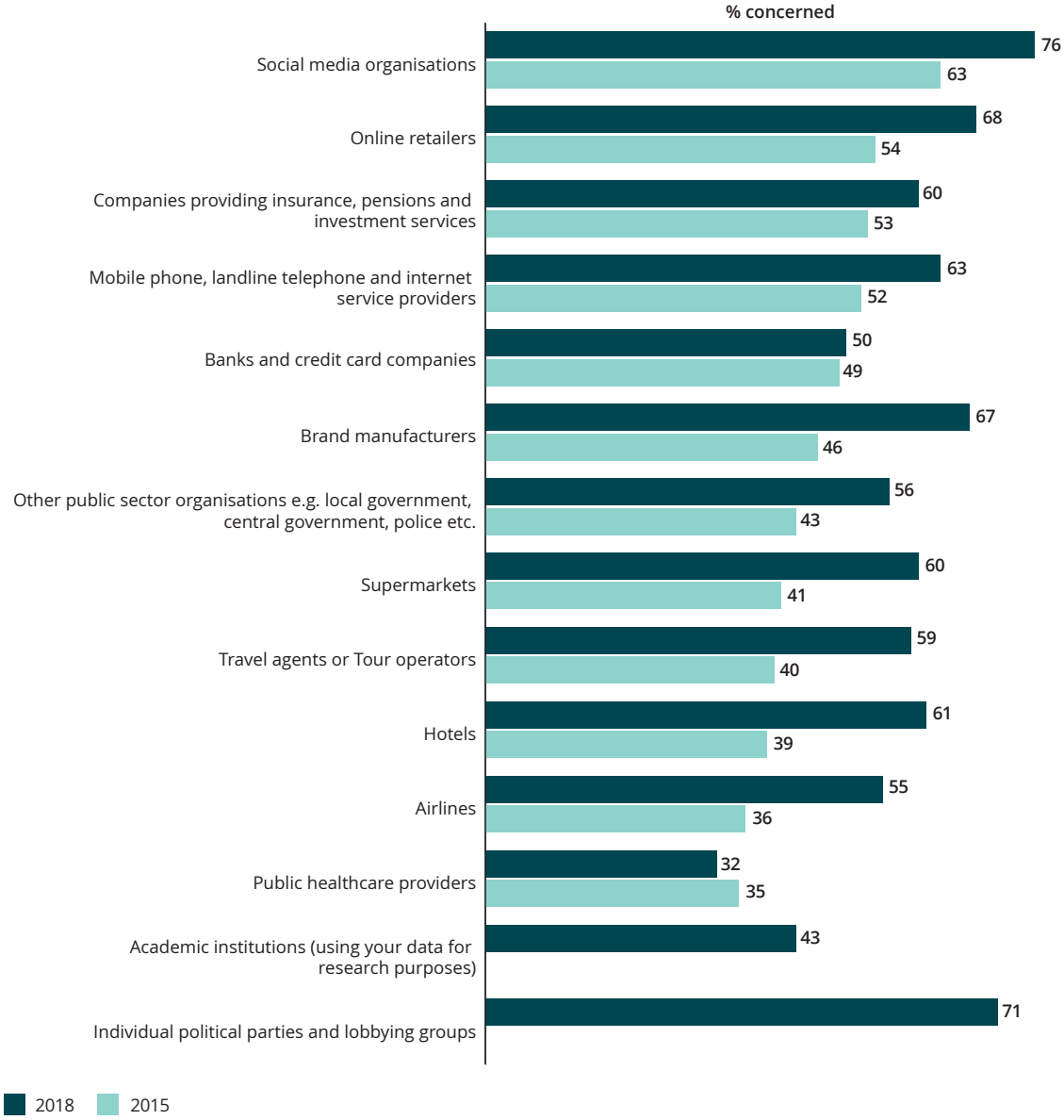
Source: Deloitte

In the three years since we last explored the misuse of data, the level of consumer concern about organisations holding or having access to their personal data has risen significantly. After some high profile incidents that have been widely reported in the media, it is not surprising that consumers have expressed concern about social media companies and individual political parties holding and having access to their data. But perhaps more concerning for consumer businesses is the level of mistrust shown towards retailers and brands.

Two-thirds of consumers are concerned about online retailers having access to their data compared to just 54 per cent in 2015, while 67 per cent are concerned about brands having access to their data compared to 46 per cent in 2015. Three-fifths of consumers are concerned about supermarkets holding or having access to their data compared to just 41 per cent in 2015. Consumers are also growing increasingly concerned about travel agents, hotels and airlines having access to their data.

Figure 6: Consumer concerns with sharing data with different types of organisation

For each of the following types of organisation, please indicate how concerned, if at all you are about them holding or having access to your personal information?



Source: Deloitte

The fact that there are already serious concerns over organisations holding or having access to personal data, means that if trust is further breached, the loss of business is a real threat. In fact, Deloitte's consumer research shows that failing to keep data safe and selling anonymous data about customers to other companies are now seen as more important reasons to stop using a company than exploiting overseas workers, damaging the environment and paying large bonuses to executives.

Figure 7: Consumer attitudes on the misuse of their data

If you found out a company you are a customer with, for example your bank or your main supermarket, was doing any of the following, which of the following would make you seriously consider not using this company again? Please select all that apply

Source: Deloitte

Rebuilding trust with consumers

Given the apparent level of mistrust, what can businesses do to restore that trust? While our data seems to suggest that consumers have lost trust in businesses, their new found awareness of the value of their data and how it is used will be viewed as an opportunity by many consumer businesses.

In light of GDPR, organisations have already begun to change the way they communicate with consumers about the use of their data. Transparency over data collection and usage can only be viewed as positive as it raises the standards that organisations are held to.

New companies with strong ethical credentials could rise to prominence, or existing organisations could champion their ethical credentials more in their marketing. Rebuilding trust with consumers will become a key priority for the majority of businesses. Those businesses that embrace this challenge and show their consumers that they have their best interests at heart have the opportunity to build longer term loyalty.

In addition to the changes in terms of marketing communications and culture, the issues we have highlighted over privacy could also drive innovation. With consumers more aware of the value of their data, we believe this will stimulate competition between consumer businesses to produce innovative goods and services that make the best possible use of personal data.

"In light of GDPR, organisations have already begun to change the way they communicate with consumers about the use of their data."

Digital risk: what does it mean for consumer businesses?

Operating in a connected, digital world presents new challenges, with new technologies and emerging digital competitors presenting new risks for businesses.

The rate of digital adoption will be different for each organisation. However, market leaders will employ new digital approaches for risk control and management, and also promote adoption of new technology across the business. In the following section we look at three areas where we believe businesses need to focus on the emerging risks that the increasing use of technology brings.

Managing risk in a digital organisation

In the digital world operations that were local are now global, manual processes are automated, organisations have constant interaction with their supplier and customers and bad news travels fast. The speed with which a risk emerges increases. Therefore businesses need to identify, manage and mitigate such risks in a productive and agile way.

Consumer businesses need to adopt a flexible and consistent approach to identifying and managing risks posed by their use of new digital technologies such as AI and machine learning across their processes, robots to interact with customers and the use of connected devices to drive sales and facilitate customer interactions. Figure 8 highlights the key risk and control considerations that businesses should consider when implementing any AI solution.

Figure 8: AI and machine learning – A risk and control toolkit

Risk categories	Key risk considerations	Key control considerations
Model	• Use and quality of algorithms	• Statistical analysis to identify and correct model bias • Appropriate feedback mechanisms • Model limitations and assumptions • Embedded key controls indicators
Technology	• Change management • Cyber-security	• Access controls • Security monitoring • Change management policies for Agile and DevOps models • Resilience and business continuity planning
Supplier	• Higher reliance on start-ups	• Supplier management framework • Business impact analysis
People	• Skills, knowledge and competencies	• AI talent strategy • Training requirements
Legal	• Data privacy and impact of GDPR and other privacy regulations • Digital compliance	• Data protection rights of customers • Global digital regulations framework
Market	• Impact on market stability	• Business continuity planning • Manual process plans documented and tested

Source: Deloitte

Managing risk digitally

Risk managers are often data rich, but struggle to extract insight and therefore value. Governance, risk, compliance and control stakeholders should embrace digital technologies to optimise efficiency, predict risk and control behaviours and generate insight on your 'control environment'. For example, new technologies require new controls processes to be put in place. Each process needs to be documented, reviewed, assessed and tested. More controls often result in more complexity and higher costs. However, while technology can create a problem it may also provide the solution, by using AI to monitor and remediate the controls library. For example, an AI assisted model would be able to identify duplicates quickly, or controls that did not comply with the documented standards, and ultimately identify gaps in the controls framework[6]. Another way in which technology can help with the management of risk is by creating a control monitoring platform that would enable real-time monitoring of multiple processes.

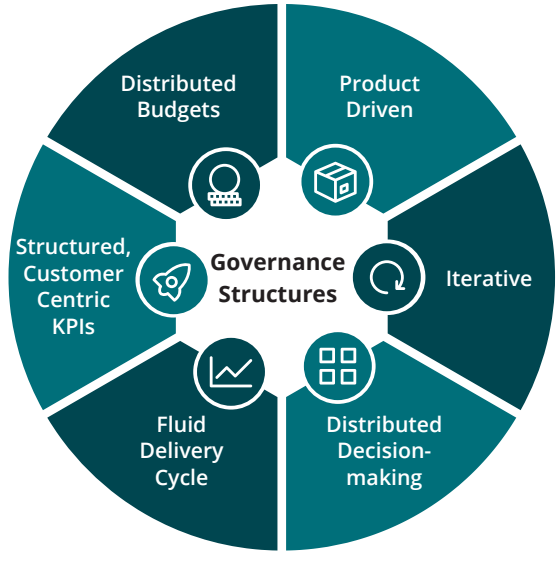
Managing digital transformation risk

Adopting new technologies requires changes to a company's ways of working. Businesses need to understand the risks of transformation to ensure they meet their objectives, while utilising the most appropriate technologies and deployment methodologies. For many years organisations have used the same approach to large transformation programmes which have typically run over a long time horizon, been rigid in structure and therefore difficult to adapt and iterate. Similarly the approach to managing the risk that business change brings has been equally fixed and is immutable. However, with large transformation programmes being replaced by the more frequent introduction of new technologies and agile ways of working, businesses need to ensure that the benefits of a faster, more agile approach are balanced by equal consideration of the risks they introduce.

Figure 9: Typical governance structure, project to product

Traditional model

Digitally enhanced model



Source: Deloitte

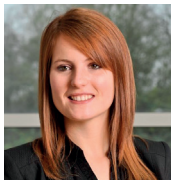
Endnotes

1. Beneath the surface of a cyberattack - A deeper look at business impacts, Deloitte University Press, 2016. See also: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html
2. Deloitte Digital Disruption Index – From experimentation to transformation, Deloitte LLP, 2018. See also: https://www2.deloitte.com/content/campaigns/uk/digital-disruption/digital-disruption/digital-disruption-index.html
3. Deloitte Global Crisis Management Survey – Stronger, fitter, better: Crisis management for the resilient enterprise, Deloitte Touche Tohmatsu Limited (DTTL), 2018. See also: https://www2.deloitte.com/uk/en/pages/risk/articles/2018-global-crisis-management-survey.html
4. Deloitte Digital Disruption Index – From experimentation to transformation, Deloitte LLP, 2018. See also: https://www2.deloitte.com/content/campaigns/uk/digital-disruption/digital-disruption/digital-disruption-index.html
5. Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office. See also: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
6. Deloitte Control Library Analysis and Remediation Assistant (Clara)

Contacts

Leadership team

André Dennis
Africa Leader, Consumer
adennis@deloitte.co.za



Charlotte Gribben
Director, Consumer & Industrial Products Digital Risk Lead
cgribben@deloitte.co.uk

Claire Hoy
Africa Director, Risk Advisory
choy@deloitte.co.za

Mike Manby
Partner, Risk Advisory
mmanby@deloitte.co.uk

Valter Adao
Africa Chief Digital & Innovation Officer
vadao@deloitte.co.za

Authors

Dr Bryn Walton
UK Research Manager, Consumer & Industrial Products
020 7007 2352
bcwalton@deloitte.co.uk

Ben Perkins
Research Director, Consumer & Industrial Products
020 7007 2207
beperkins@deloitte.co.uk

Notes

Deloitte.