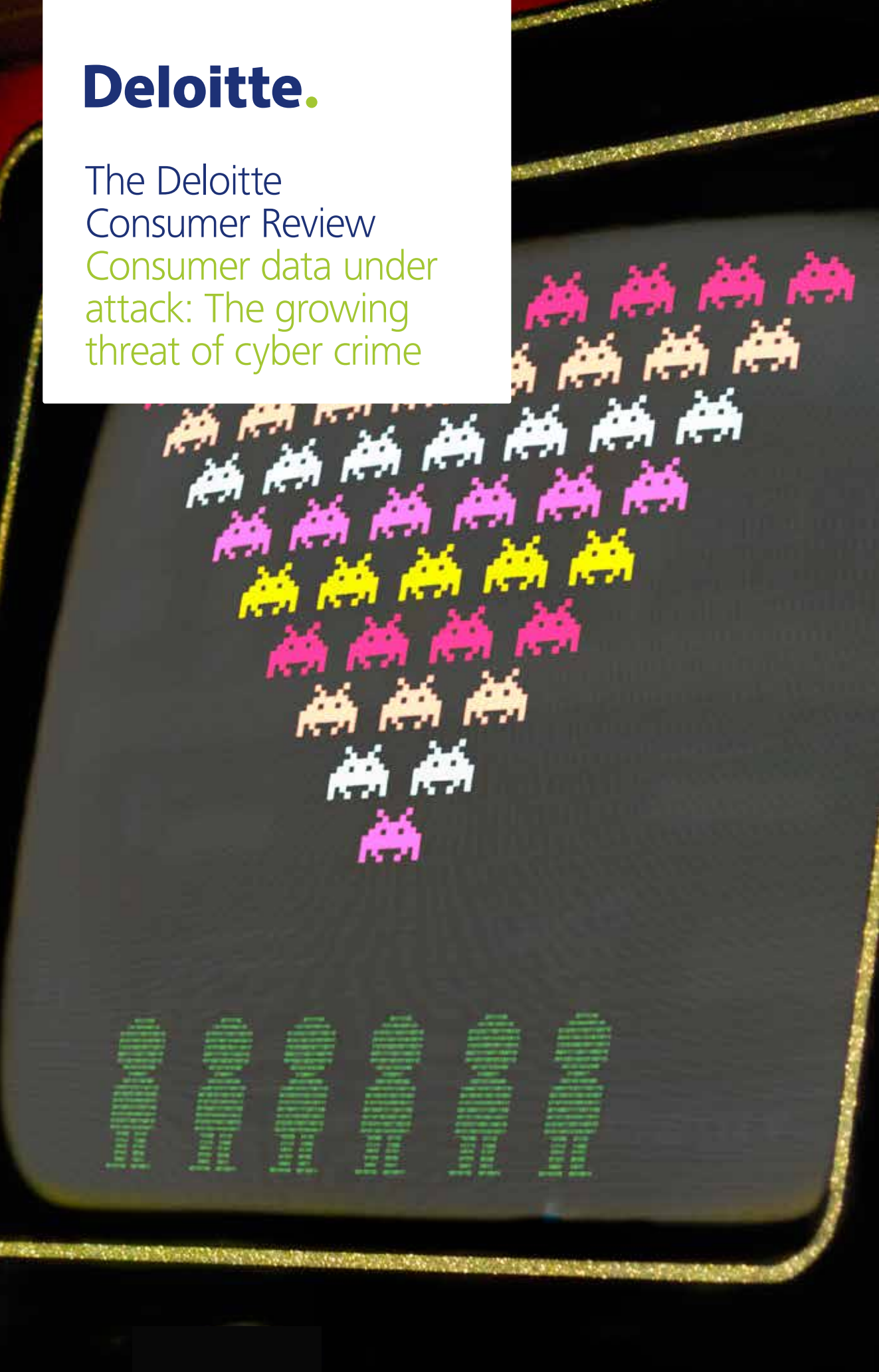
Deloitte.

The Deloitte Consumer Review

Consumer data under attack: The growing threat of cyber crime



Contents

About this research

The research featured in this report is based on several consumer surveys carried out by independent market research agencies on behalf of Deloitte.

The 2015 data is based on a survey that was conducted online with a nationally representative sample of 1,467 GB adults aged 18 to 64. The fieldwork was undertaken between 11th and 14th September 2015.

The 2014 data is based on a survey that was conducted face-to-face with a nationally representative sample of 1,537 GB adults aged 18 to 64. The fieldwork was undertaken between 11th and 21st April 2014.

The 2013 data is based on a survey that was conducted online with a nationally representative sample of 2,018 GB adults aged 18 to 75. The fieldwork was undertaken between 15th and 18th January 2013.

Please visit http://www.deloitte.co.uk/consumerreview for additional content related to the Consumer Business industry.

Foreword

Welcome to the latest edition of the **Deloitte Consumer Review.** This edition focuses on cyber crime and security for consumer businesses.

The potential for cyber crime has grown dramatically over the past few years as cyber criminals constantly adopt more profitable, effective and efficient tactics. Cyber crime is on the rise, not only in the number of attacks but also in its severity. In the UK cyber crime costs businesses £34 billion per year, including £18 billion from lost revenue.* In our experience, 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.

At the same time, major technological developments are challenging the way businesses compete and operate. Businesses' digital activities continue to grow due to the digitalisation of operations and functions. Not only are businesses collecting more data they are also becoming increasingly dependent on it for their day-to-day operations. In a world where cyber crime is becoming ever more attractive, businesses are exposed to more security risks than ever before.

Our research shows that as a result of the increase in cyber attacks, consumers are becoming more distrustful about how secure their data really is when sharing their personal information with businesses. This lack of trust provides an opportunity for businesses to act transparently and reassure consumers that their data is safe with them. Businesses need to be explicit not only in how they secure consumers' data, but also in the benefits to consumers of sharing their data and in giving them the choice about how their data is used.

Together, these issues illustrate why cyber-security risks have become a priority for leaders in business and why now is the time to act to ensure that effective cyber-security measures form part of the business strategy.

We hope this report gives you the insight and data to enhance your understanding of the opportunities and challenges in your sector, and welcome your feedback.

Nigel Wixcey
Partner, Consumer Business, Deloitte LLP

*The Centre for Economics and Business Research

Executive summary

The more data a business collects about its consumers and the more sensitive that data is, the greater the data's attractiveness to cyber criminals. With businesses becoming more and more dependent on data to manage their operations, the risks of cyber crime can only get greater. Although consumers tend to get caught in the middle, they are not always the prime target. Some criminals want to benefit financially; others want to damage a company's reputation. This makes the risk of cyber crime not just an IT issue but a business issue as well.

While boards are becoming more aware of cyber risks they are still struggling to comprehend the full impact a cyber incident can have on their own organisation and strategy. To overcome this, businesses need to develop an integrated approach to cyber security with board-level accountability, one that links business objectives to security priorities and helps to create a common language between technologists and business leaders. The approach needs to be set at the top, with the board, CEO and the CFO setting the governance and organisational structure and ensuring all employees understand their role in preventing cyber attacks. Business leaders need to incentivise collaboration, and consider creative ways to raise awareness across the organisation through activities such as war-gaming, to help create the right security culture.

Businesses need to take the lead in fighting cyber crime especially when considering their consumers' experiences and attitudes to cyber crime. Our research shows that consumers are experiencing a growing level of security breaches, particularly around fraud and theft. There is also a certain degree of scepticism, even cynicism, among consumers regarding corporate motives and practices around the collection and use of personal data. Indeed our data points to a decline in consumers' trust in the ability of businesses to secure their personal data and use that data appropriately.

As a result consumers are taking more control over securing and sharing their data, and are increasingly willing to withdraw consent if they do not perceive the right protections are in place. Compared to our research results in 2013, the proportion of consumers that 'did nothing' following a cyber-security breach has dropped significantly.

Our research also suggests, however, that businesses may be over-estimating not just consumers' comfort with sharing their personal data, but also the extent to which consumers are satisfied with what they are receiving in exchange for that data. Customer experience will be the primary basis for competitive differentiation in the next few years. This presents an opportunity for consumer-facing companies to develop strong cyber-security strategies that can generate a competitive advantage, including reassuring consumers and acting transparently about how personal data is managed and used.

Cyber-security risks will only intensify as businesses focus their investment on acquiring more analytics tools and basing more and more of their interactions with consumers in the digital space. While the amount of data accessed and shared across an ever more complex network increases, companies need to sharpen their focus and ensure they protect one thing: the trust of their customers – consumers and businesses alike. In both instances businesses need to make sure their customers are totally confident that their data is managed and used in the most secure way possible.

In summary, data usage and security practices are not just about risk mitigation, they are also a potential source of competitive advantage.

Consumer trust is eroding

73% of consumers would reconsider using a company if it failed to keep their data safe.

Yet only **51%** would switch companies if they were charged a higher price than competitors for a similar product.

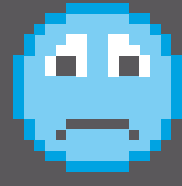
Doing nothing is no longer an option

More consumers have experienced a cyber breach in 2015 than in 2013, yet today, fewer are **doing nothing** as a result.

1/3 of consumers would now close their online account following a breach or stop dealing with the business they think is responsible.

32%
Happy for my information to be used

54%
Not happy for my information to be used



*14% don't know.

A fair exchange

Despite companies being able to offer a personalised or better service via personal data, most consumers are still not happy with their information being used.

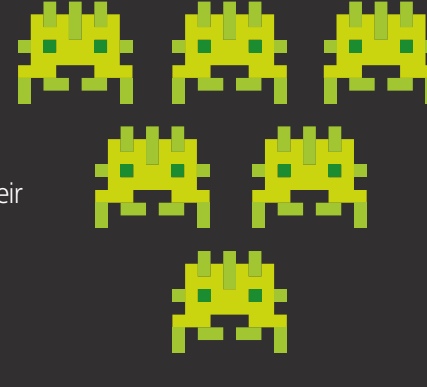
66% of consumers would ask companies to remove their personal data if it was easy to do so.

Bringing cyber to the board

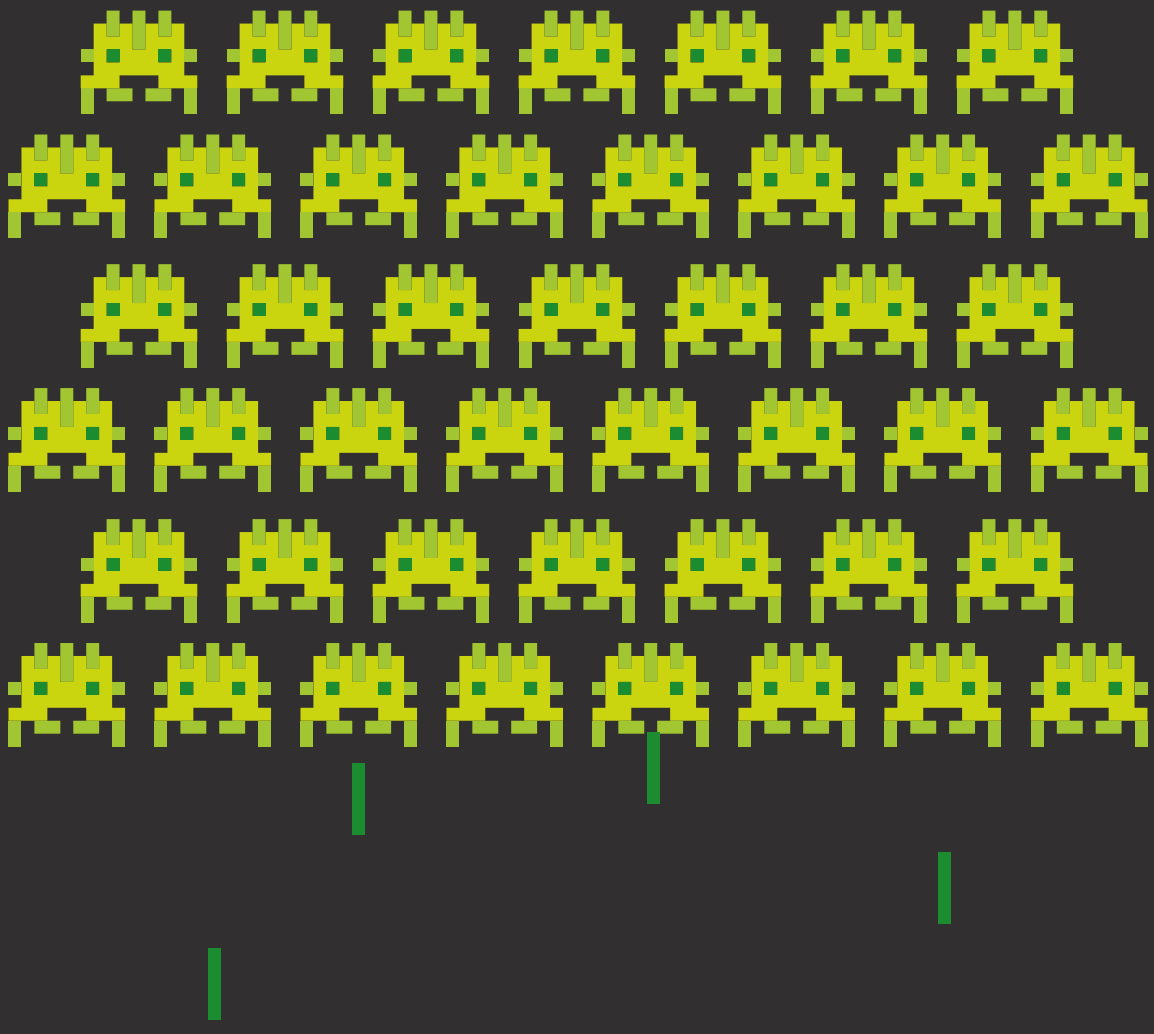
Cyber crime costs British businesses

£34bn a year*

Not just an IT issue, boards need to take note of consumers' **awareness** and **cynicism** about how their data is used. Building the right cyber strategy, with transparency at the heart, could lead to gaining **competitive advantage.**



*Centre for Economics and Business Research.



Consumer data under attack

As more of their assets become digital, the risks and implications of cyber attacks are intensifying for businesses in the consumer sector.

Our research highlights that security concerns are causing a reduction in consumer activity as consumers avoid sharing personal data with businesses to protect their privacy. Our research also shows that more than one in three consumers who have experienced some kind of security breach will voluntarily cease any dealings with the business they think is responsible.

However the data also shows that businesses have an opportunity to use data protection and customer privacy to gain competitive advantage, by educating and reassuring consumers that their data is held securely. Three in four consumers think it is the responsibility of companies to provide them with the tools they need to protect their privacy, security and reputation, while 57 per cent are also more likely to use or recommend a company that lets them decide how their personal data is used.

This shows that businesses need to turn data security to their advantage by ensuring policies and procedures are robust. Businesses need to be transparent with consumers in how their personal data is managed, secured and used. Businesses also need to communicate to consumers the benefits of sharing their data to encourage them to continue to do so.

In this section we review our consumer research findings, which can be summarised under the following themes:

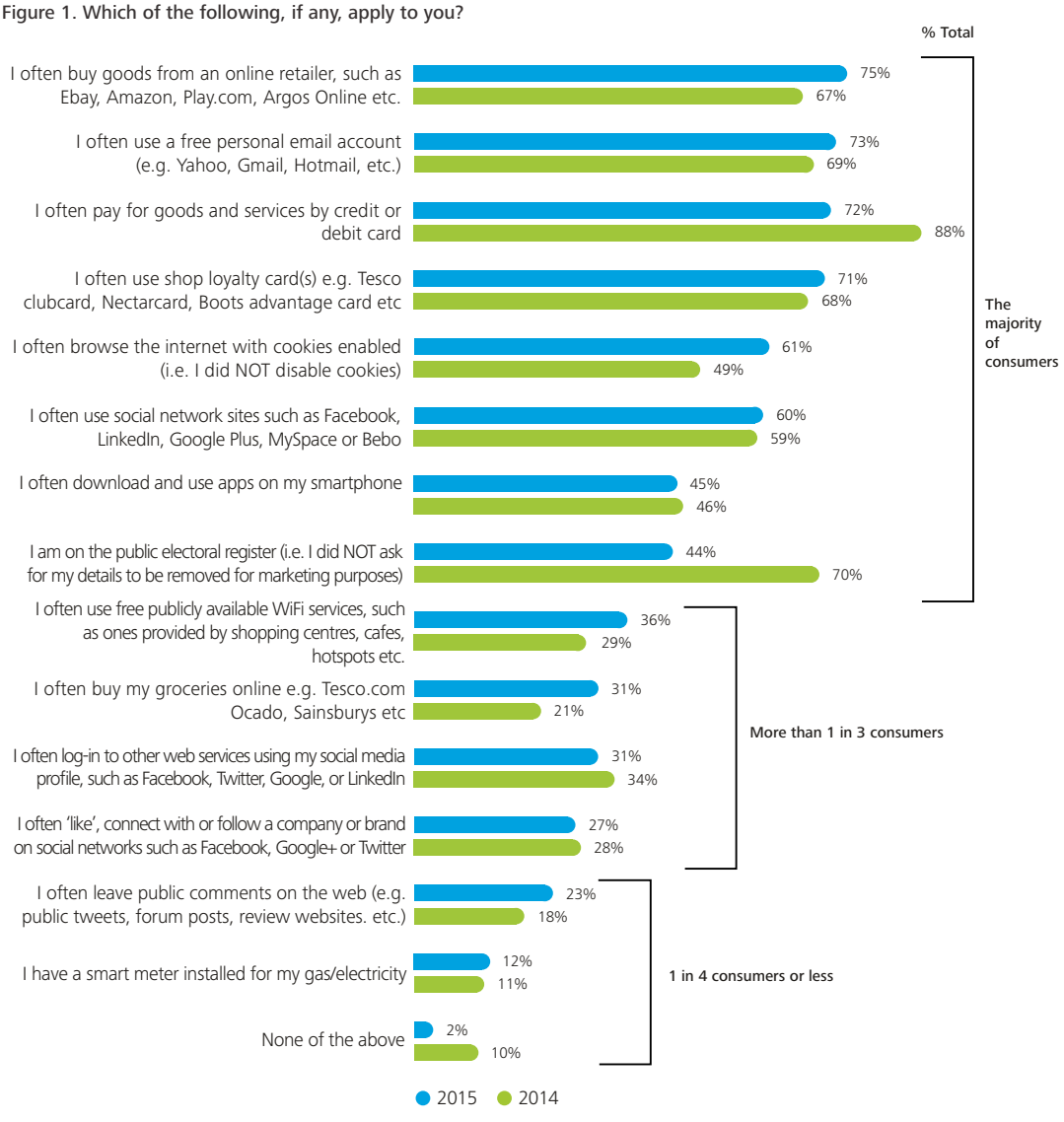
- an increasingly driven data nation
- growing consumer awareness about data usage
- consumers' experience of cyber crime and their attitude to data security
- the issue of trust
- consumers taking control
- the need to state explicitly what consumers get in exchange for sharing data
- changes in regulations giving more power to consumers.

An increasingly data driven nation

Deloitte's research indicates that consumers' digital footprint is increasingly driven by purchasing activities. The data shows that in 2015 there is a higher proportion of people buying goods and services online than using email accounts. While this type of transactional data presents an ever increasing opportunity for businesses, it is also appealing to criminals and therefore increases the risk of a cyber attack.

The data shows there is also a growing proportion of people browsing the internet with cookies enabled compared to a year ago. This could mean that either people are becoming more comfortable with their data being used and tracked or they are paying less attention to cookie acceptance messages (see Figure 1). This trend was particularly strong among younger age groups who tend to be less concerned about sharing their data than older groups.

Figure 1. Which of the following, if any, apply to you?



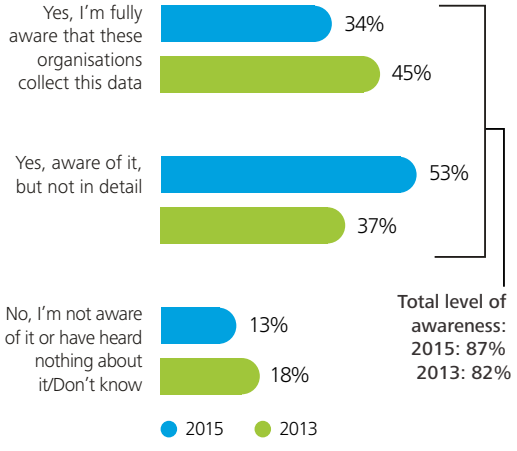
Base: All GB adults aged 18 to 64, 2015 (n=1,467) 2014 (n=1,537)
Source: Deloitte research

Growing awareness about data usage

Consumers still do not understand how much data companies hold about them. The research shows that total level of awareness about data being collected and stored by businesses has gone from 82 per cent in 2013 to 87 per cent in 2015. Yet there is a growing misunderstanding of what data is being stored by whom. A higher proportion of consumers (53 per cent) claim they do not know the details of what data organisations have collected about them and their activities compared to 2013 (37 per cent) (see Figure 2).

Figure 2. Awareness of personal data stored by third parties

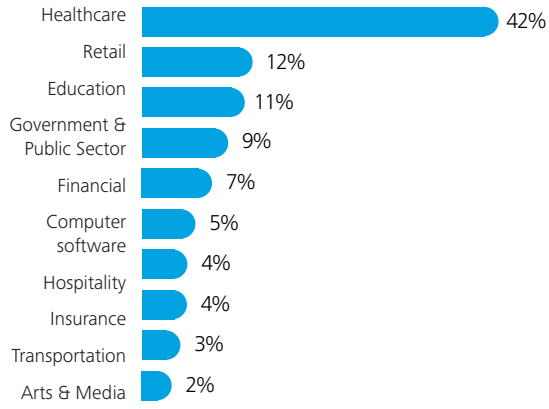
To what extent are you aware or not that companies and public sector bodies collect data about you and your activities?



Base: All GB adults aged 18 to 64, 2015 (n=1,467) 2013 (n=2,018)
Source: Deloitte research

When it comes to consumers' concerns about data usage in different sectors, the level of concern about the private sector is, on average, much greater than about the public sector. This is despite the fact that a smaller percentage of all data breaches reported originated from sectors such as retail. This sector suffered 12 per cent of all incidents reported in 2014 compared to 42 per cent in the healthcare sector in the same period (see Figures 3 and 4).[1]

Figure 3. Top ten sectors breached by number of incidents

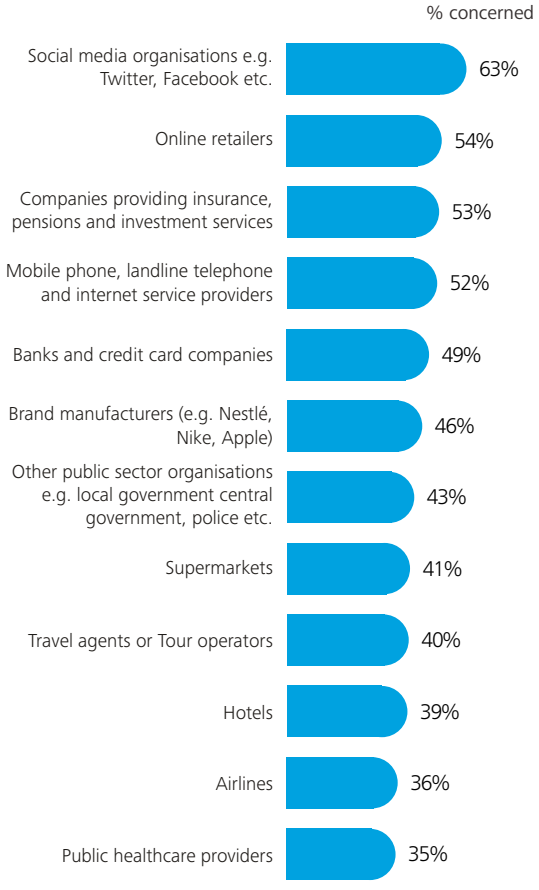


Source: Symantec

Consumers are most worried about social media companies, online retailers and financial services organisations having access or holding their personal information. This apparently contradictory finding could be related to the more transactional relationship between consumers and the private sector. This highlights the importance of businesses being transparent not only in how they use consumers' personal information, but also in how they communicate the potential benefits to consumers of sharing their data.

This also highlights the importance of the consumer sector industries being more open in sharing their experiences. Businesses could benefit from greater collaboration across the industry, as well as with government, to protect the industry as a whole, despite competitive interests. Businesses need to agree a coordinated response on how to manage the risks of cyber attacks.

Figure 4. Level of concern by type of organisations



Base: All GB adults aged 18 to 64, 2015 (n=1,467)
Source: Deloitte research

An escalating risk

Consumers' growing concerns correlate with their increasing experience of cyber crime. Our research shows that there is a significant increase in the proportion of people having experienced some form of cyber-security breach since 2013. The most significant increases have been in breaches related to fraud and theft. The data shows that one in five consumers has suffered a financial loss as a result of a cyber-security breach (see Figure 5).

Official data also shows the growing threat of cyber crime and online fraud. An estimated 3.8 million adults in England and Wales were victims of some form of online fraud in the year ending June 2015, according to figures in the Crime Survey for England and Wales. The official survey found an estimated 5.1 million incidents of online fraud and an estimated 2.5 million incidents categorised under the Computer Misuse Act, where the victim's computer or other internet-enabled device was infected by a virus or where a victim's email or social media account had been hacked.[2]

Figure 5. Consumers' experience of security breach (2013 vs 2015)

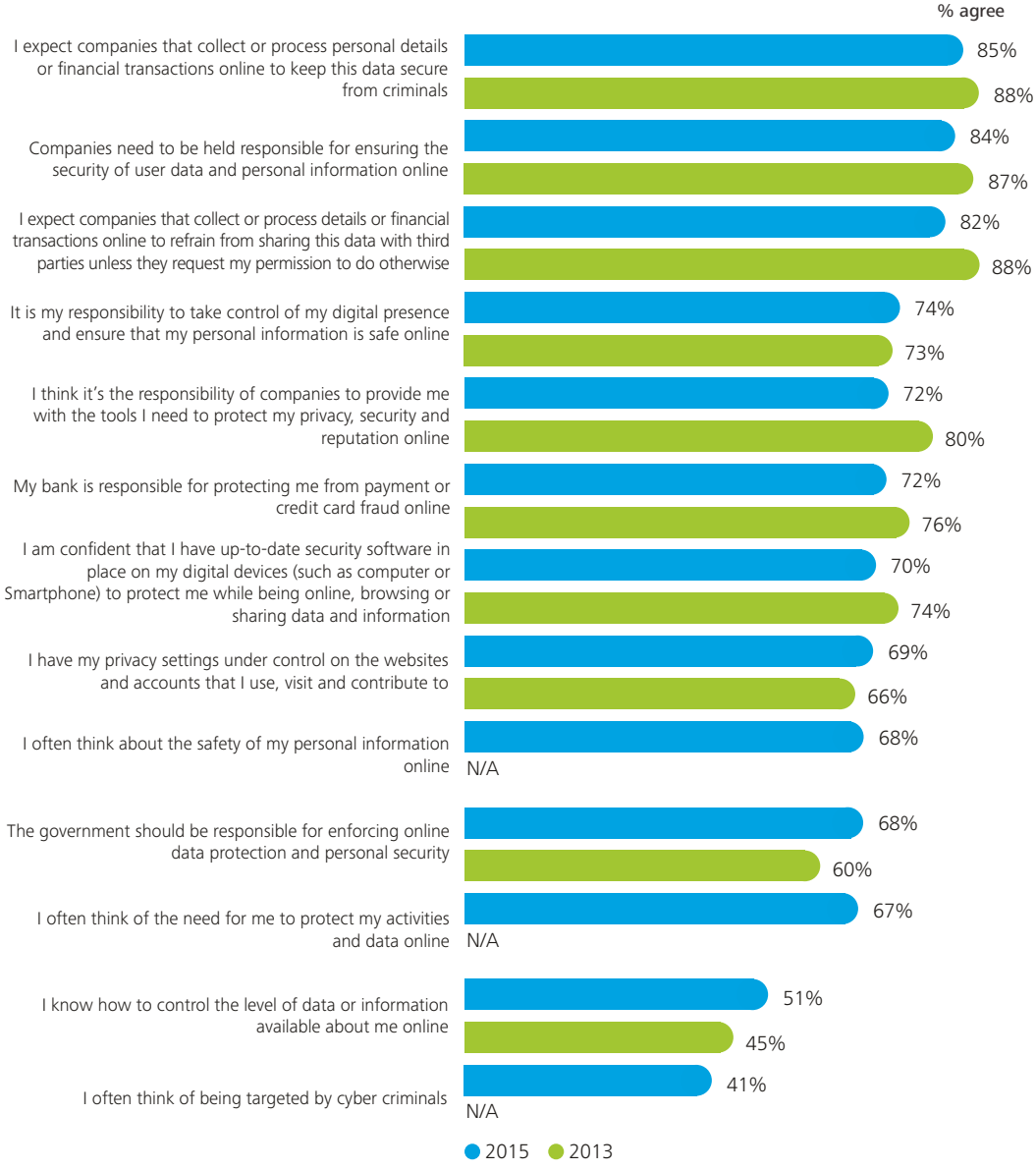
Thinking about any online security issues that you might have been affected by, how often, if at all, have you experienced any of the following?

Base: All GB adults aged 18 to 64, 2015 (n=1,467) 2013 (n=2,018)
Source: Deloitte research

There is a general shift towards consumers being more proactive and believing that they should take responsibility for protecting their data online, rather than relying on others, such as companies, government or their bank, to do it for them (see Figure 6). This erosion of trust combined with more empowered consumers will continue to challenge businesses in how they communicate with consumers around personal data management as well as what tools they will provide their consumers to secure that data.

Figure 6. Consumer attitudes to data security

Thinking about the security of your personal data, to what extent do you agree with the following statements?



Base: All GB adults aged 18 to 64, 2015 (n=1,467) 2013 (n=2,018)
Source: Deloitte research

An issue of trust

Unsurprisingly, given the increase of security breaches consumers have experienced, the public's confidence in their data being handled securely or analysed for their benefit has remained consistently and worryingly low for the last two years. Four out of five measures of confidence have dropped in 2015 compared to 2014 (see Figure 7).

However, there are two ways of looking at these results. On the one hand, our research describes a largely uncertain, untrusting public: a national population that begrudgingly gives up its data and all control over it while remaining deeply cynical about the commercial motives of the organisations using it. On the other hand, this lack of confidence provides a new opportunity for organisations to offer greater transparency, more tailored benefits and cede control of personal data back to consumers.

Figure 7. Level of trust in how companies use data

How much confidence, if any, do you have in the following?

Base: All GB adults aged 18 to 64, 2015: (n=1,467) 2014: n=(1,537)
Source: Deloitte research
*Please note that the 2015 data comes from an online survey and 2014 data comes from a face to face survey

Consumers are very clear in their message to businesses and third-party organisations: the number one issue that would make consumers reconsider using an organisation is if that organisation lost their data or failed to keep it safe. That applies to a large proportion of consumers (73 per cent) and is higher than the proportion of consumers who would reconsider using an organisation if they were charged a higher price than the competition for an equivalent level of service or product. It highlights the value consumers put on their personal data being kept secure (see Figure 8).

Figure 8. Consumers' trust threshold

Which of the following would make you seriously consider not using a company again?

Base: All GB adults aged 18 to 64, 2015 (n=1,467)
Source: Deloitte research

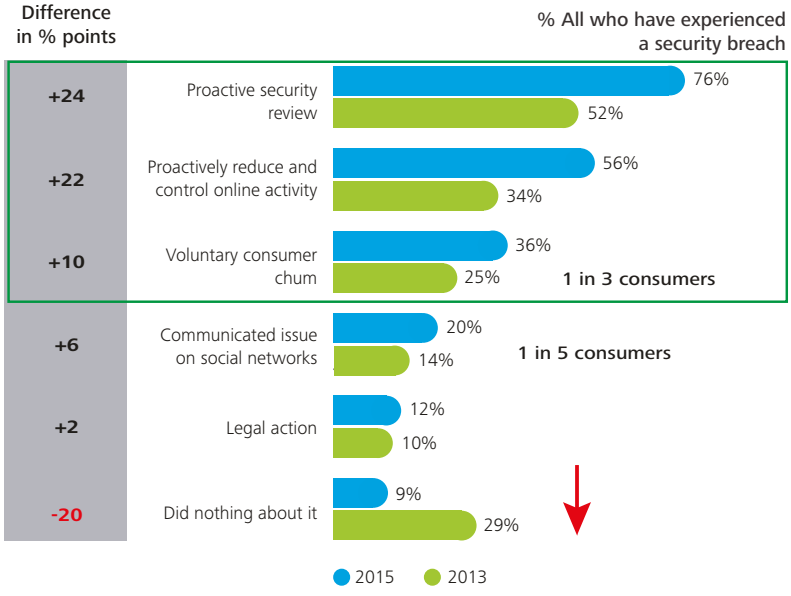
Consumers take control

As a result of their growing experience of security breaches and their mistrust in organisations' ability to keep their personal data secure, consumers are taking matters into their own hands. There has been a significant increase in the proportion of people taking actions following a security breach, with the majority proactively going through a security review, and controlling or reducing their online activity. Moreover, one in three consumers closed their account and stopped dealing with the business they felt was responsible for the breach.

Consumers are really starting to understand the impact a security breach can have on them; hence the significant decline in the number of people doing nothing following being victim of a breach (see Figure 9).

Figure 9. Behaviour following a security breach

Following the online security breach or threat you have just listed, which of the following steps have you taken, or will you take, as a result of this event? Select all that apply.



Base: All GB adults aged 18 to 64 who have experienced a security breach, 2015
Source: Deloitte research

Proactive security review
- Changed passwords
- Created a new email address account(s) and deleted existing email account(s)
- Upgraded my antivirus and/or security software
- Changed my antivirus and/or security software
- Taken steps to identify and use online services who promise increased levels of security
- Contact the site where the incident occured/originated

Proactively reduce and control online activity
- Reduced the amount of time you spend online
- Reduced the amount of activities you do online (e.g. less online shopping, or a reduced amount of film streaming).
- Take greater care in controlling the amount of personal data that exists online

Voluntary customer churn
- Closed my online shopping account
- I stopped dealing with the website I think is responsible for compromising my data

Communicated issue on social networks
- Warned others on social network sites and forums

Legal action
- Took legal action (e.g. reported the incident to the police)

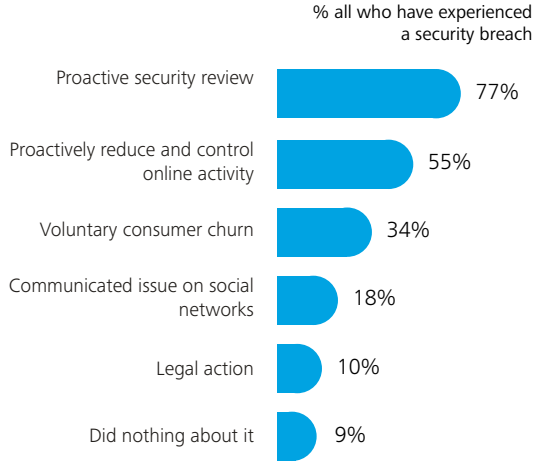
Nothing
- Do nothing about it

All the evidence from Deloitte points to the need for organisations to be transparent, and to act quickly when they realise their consumers' data has been breached. However there can be a conflict of interest for businesses: one in three consumers say they will voluntarily stop dealing with a business if they are informed of a breach, even if they do not suffer a material loss. Yet recent examples have shown that the impact is much worse if the response is not authoritative, timely and transparent (see Figure 10).

Companies also need to make provision for consumers to take control of their security before they suffer a breach. Prevention and empowering people to take control should come first. For example Google has been proactively reminding consumers around how to manage their privacy better through the creation of a single hub called 'My Account'. It subdivides the settings into three sections: sign-in and security, personal info and privacy, and account preference allowing consumers to switch a number of features on or off.[3]

Figure 10. Behaviour following a breach where no material loss occurred

I have been notified that my account details have been stolen but no fraudulent activity has taken place.



Base: All GB adults aged 18 to 64 who have had their account details stolen but no fraudulent activity has taken place, 2015
Source: Deloitte research

A fair exchange

The data shows that the majority of consumers are still not happy with their personal information being used even if it means they could get personalised products or services or help to improve products or services. One of the reasons why consumers might not be so confident in companies using their personal information and data to offer them a better level of service or more personalised products is that businesses do not always clearly tell consumers what the benefits of sharing their personal data with them are (see Figure 11).

Figure 11. Consumers' level of comfort with companies using their data

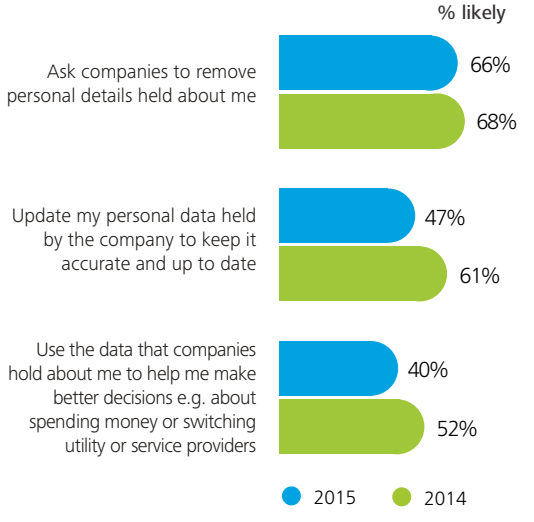
We are now going to show you some different scenarios about how personal information can be used by organisations. For each of these, please indicate which of these two statements comes closest to your own opinion.

Base: All GB adults aged 18 to 64, 2015 (n=1,467)
Source: Deloitte research

As a result, if businesses made it available, more than half of consumers would ask for their data to be removed (66 per cent) and fewer would update their personal data to keep it accurate (47 per cent in 2015 compared to 61 per cent in 2014). An even lower proportion would use the data held by companies to make better purchasing decisions (40 per cent in 2015 compared to 52 per cent in 2014) (see Figure 12).

Figure 12. Consumer attitudes to managing their data if made possible

If companies or organisations made it easier for you, how likely or unlikely would you be to do the following things?



Base: All GB adults aged 18 to 64, 2015 (n=1,467) 2014 n=(1,537)
Source: Deloitte research

Businesses handing over more control to consumers in deciding whether and how their data is used should benefit from increased levels of engagement, but as the data demonstrates, businesses may also face increased risk of consumer disengagement if that control is not backed by strong consumer trust. At the moment consumers do not trust how companies use their data and do not understand what type of data is being held about them, and as a result will prefer to opt out from their personal data being used.

In the absence of trust and transparency, the relationship between consumers and businesses might become a race to the bottom on price. Building trust therefore becomes a way for an organisation to avoid margin-erosion.

This overall decline in consumers' engagement also demonstrates that they are less prepared to collaborate as they do not see the real benefits of doing so. When it comes to their data, today's digital consumers are savvy and discerning. This means that businesses can no longer afford to compete solely on the basis of more traditional values. Product innovation, value-for-money, quality, service offerings and convenience remain vital elements of a proposition that now includes trust in the way that personal data is handled and the motives for its use. Consumers engaged under the principles of transparency, clarity and data security are more likely to stay.

The upcoming European Commission (EC) regulation on data protection and privacy – the General Data Protection Regulation (GDPR) – will introduce four new dimensions aimed at giving consumers more control in protecting their data. The regulation, which could come into effect in 2017, includes the following measures:

- **Consent –** companies will be required to get consumers' consent to use their personal data.
- **Breach notification –** companies will need to notify consumers affected without undue delay when their data has been breached.
- **Right to be forgotten –** consumers will have the right to ask companies to erase any personal data they hold about them and stop companies from sharing that data with anyone.
- **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.


GAME
OVER

A cyber-security strategy fit for purpose

Cyber-security threats continue to change both in terms of frequency and sophistication.

As a number of forces converge, the risk of wider and more powerful cyber attacks on businesses is intensifying. In this section we explore how cyber attacks have evolved and how they are changing the nature of risk and forcing businesses to rethink their cyber-security strategy.

Digital disruption

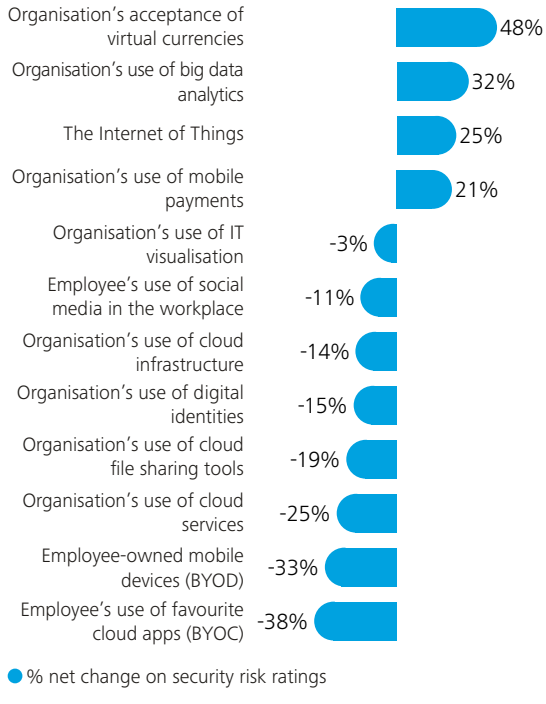
The rapid expansion of the connectivity of things and people in the digital space shows no signs of slowing. For example, while the internet is powered by people using search engines, browsing and shopping online, the future will be powered by smart objects connected with each other and able to share information in the so called 'Internet of Things'. In addition to their more traditional engagement through transactions or loyalty schemes, consumers are now signing up, checking in, 'liking' and engaging with businesses on social media. These new relationships are providing businesses with an unprecedented amount of insight and data about consumers' behaviours and preferences.

As a result more data is being exchanged and shared than ever before. Trends contributing to this influx of data include the growing usage of social media, the rise of mass personalisation, the 'Internet of Things', contactless payment solutions such as mobile payment or the peer-to-peer payment industry, manufacturers selling direct to consumers online and the rapid expansion of global e-commerce activities.

As data is created and transmitted across wider and more complex networks, there is an increasing risk that that information could be compromised at a time when businesses' dependence on accessing that data in real time has become critical to their operations.

It also raises new security complexities and widens the issue of cyber-security governance. More data and more sensitive data, available across a broader network mean the risk of a security breach is higher. According to data from the Ponemon Institute, the increasing use of virtual currencies, data analytics, the Internet of Things and mobile payments will increase the risk of security breaches. Yet not all disruptive technologies will increase the risk. For example, the use of robust, centrally provisioned digital identities will actually help to decrease it (see Figure 13).[5]

Figure 13. Impact of disruptive technologies on the risk to an organisation

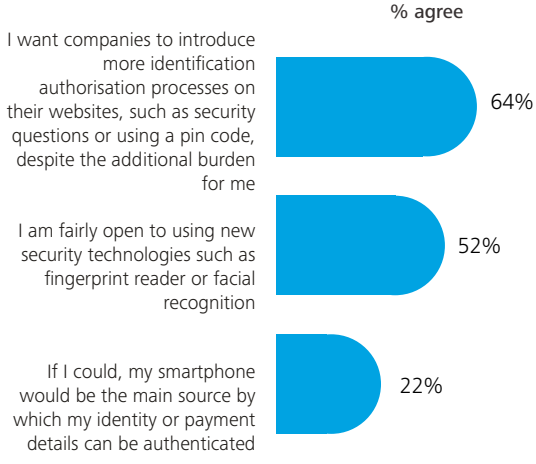


Source: Ponemon Institute, February 2015

Increasing business interactions with consumers in this new digital space will result in a drive for the use of advanced authentication. Successful systems will be more intuitive and provide a seamless experience where users no longer need to memorise a number of complex passwords for example. Our research shows that one in five consumers would be happy for their mobile device to be used as the main means for authentication. Consumers are also open to newer, more rigorous technologies, but they are increasingly unlikely to accept such technologies if they disrupt their shopping journeys (see Figure 14).

Figure 14. Consumer attitudes to authentication

To what extent do you agree or disagree with the following statements?



Base: All GB adults aged 18 to 64, 2015 (n=1,467)
Source: Deloitte research

The changing nature of cyber crime

Cyber crime is undeniably on the rise and remains a growth-industry. For example, the advent of the so-called 'cyber-crime-as-service' (CaaS) business model – where attackers have easy access through underground forums and black markets to tools – has enabled a large number of unskilled and aspiring criminals to launch sophisticated attacks on businesses and individuals alike.

The digital underground marketplace has evolved and matured into a thriving cyber-criminal industry globally that costs global economies more than US$300 billion per year. In the UK, the Centre for Economics and Business Research estimates that cyber crime costs British businesses £34 billion per year, including £18 billion from lost revenue.[6] However, the true cost to the UK and other countries is likely to be much greater, due to the continued reluctance of both businesses and individuals to report these crimes. It is difficult to place a value on stolen data and therefore also difficult to quantify accurately the cost to businesses. However it has been estimated that the cost of intellectual property theft through cyber crime is as high as 0.9 per cent of GDP in high income countries such as the UK. As a result, some businesses either overspend or misdirect their spending on data protection. If there was more disclosure, and thus more information on the amount, types and costs of cyber crime, companies would be in a better position to spend their information-security budgets.

The globalisation of e-commerce

In today's increasingly digitalised world, the global marketplace has welcomed the growth of e-commerce as a cost-effective solution that facilitates growth and the delivery of goods, to an increased consumer base. E-commerce has revolutionised traditional business models and business transactions, creating huge growth opportunities for a wide range of sectors and industries.

The sheer size of the global e-commerce market – estimated to be worth US$1.2 trillion per year – makes it a prime target for cyber criminals. An estimated US$3 billion of revenue is lost each year to cyber crime.[7] The use of the internet as an intrinsic component of e-commerce has meant that online businesses and e-commerce platforms are exposed to a wide range of cyber-related risks due to the potential for malicious attackers to gain access to Personally Identifiable Information (PII) relating to consumers, alongside financial data including transaction details and credit card numbers.

Taking down websites

Fraudulent websites are commonly used by cyber criminals in phishing attacks to obtain information (usually credentials or credit card details) from their targets. They can also be used as a front for the sale of counterfeit goods including designer brands. Our research shows that 66 per cent of consumers have received phishing emails and 38 per cent have gone onto phishing websites (see Figure 5).

Identifying and taking down malicious websites are key to reducing phishing attacks and the sale of counterfeit products. Where fraudulent sites are identified as being malicious, a cease and desist notice can be sent to the internet service provider for the host in question, calling for the malicious site to be removed due to its association with illegal activity. However, attackers can make this difficult by frequently hosting their phishing sites in countries with limited law enforcement capabilities.

According to the Anti-Phishing Working Group (APWG), 123,741 unique phishing attacks were reported to them in 2014, which included 22,679 maliciously registered domains, targeting 756 organisations.[8] The most targeted industry was the e-commerce sector (32.4 per cent of all attacks), with Apple the most targeted organisation (17.7 per cent). Given that these websites were reported, it is likely that attempts were made to take the sites down, although the report does not confirm the number of successful takedowns. It is crucial that websites are taken down promptly as most visits to a fraudulent website are made within the first 24 hours of uptime. While the average uptime reported by the APWG for fraudulent websites was 32 hours 32 minutes, over half of the websites had an uptime under nine hours.

In its weekly transparency report Google reported that for the week beginning 4 October 2015, 25,757 phishing websites were detected by their Safe Browsing Technology indicating that many potentially fraudulent websites are not reported.[9] It is extremely difficult to assess how many websites are taken down on an annual basis, as many different organisations and hosting companies are involved in the process and many individual victims do not report their attacks. In 2014, 2,500 websites selling counterfeit designer goods were taken down by the Police Intellectual Property Crime Unit in the UK.[10]

Given the importance of trust between consumers and businesses, prompt detection, disruption and takedown of fraudulent websites remain key priorities in minimising the impact of online fraud on both consumers and targeted businesses. However this requires effective reporting and the cooperation of associated internet hosting companies.

In addition to building trust with consumers with their direct-to-consumer propositions, consumer product manufacturers will also be interested in brand protection. With the increasing number of fake websites and fake goods being sold online, brand protection is critical.

The right security culture, capabilities, governance and technologies

Changes in security strategies are driving a number of key imperatives including:

- given the growing complexity of the risks and the threats, cyber security requires not just the right technologies to counter cyber crime, but also the right enterprise-wide strategy
- the strategy needs to recognise that cyber security is not 'an IT problem' but a broader business and cultural problem
- companies need to be more joined up across all their go to market channels in the way they manage their data security risks.

Many organisations are struggling to deliver effective cyber-security protection and response capabilities as they have seen the solution as purely a technology one. However, in our view, effective security capability must be built around an understanding of the risks, then integrated into every business process, and executed by people with the right skills and knowledge. Technology can be the enabler of this execution, by providing scale and efficiences, but it is not a substitute for it. Effective management is a challenge for all organisations as they continue to adopt online technologies and new channels of delivery.

These challenges in delivering effective security capabilities are exacerbated by cyber-talent shortages, budget constraints, the increasing complexity of business and IT environments, and information overload of alerts from security technologies and threat intelligence. While an organisation's defences against cyber attack are dependent on having the right security culture, the success of the information security function relies on a clear understanding, allocation and ownership of risks, roles and responsibilities.

Building a mature cyber-risk culture across all layers of an organisation, combined with an enterprise-wide strategy, are essential to mitigating cyber-crime risks successfully.

Change in the regulatory environment and implications

The European Commission is in the process of overhauling EU data protection legislation with the proposed introduction of regulatory requirements that are likely to impact businesses across all sectors. While the reform is focused on improving consumer protection, current proposals seem likely to result in extra burdens and restrictions for businesses.

With the rules set to change, businesses are likely to face a variety of new technical and procedural challenges. If businesses fail to act early they could struggle to align policies and procedures with the new requirements. This could result in fines for non-compliance, reputational damage or missed opportunities to demonstrate to customers that the business treats their data responsibly.

Proposed changes and potential impact:

Proposed requirement	Description	Potential impact
Right to data portability	Where personal data are processed by electronic means and in a structured and 'commonly used' format, they must be provided to an individual in a 'commonly used' format upon request.	• Impacts across all business units, including data processors. • Divergent, highly segregated systems are unlikely to be compliant.
Breach notification	Notification of a data breach to the supervisory authority and to the data subject within a specified timeframe.	• Impacts across all business units, including third parties. • Incident management procedures will need to be updated.
Transparency	Policies relating to data protection should be transparent and easily accessible.	• Impacts data capture forms across a variety of on and offline media platforms. • Privacy policies will need to be updated.
Privacy by design	If a processing operation presents a specific risk to the rights and freedoms of individuals, the controller must carry out auditable Privacy Impact Assessments.	• Impacts project development lifecycle. • Tools and templates will be required to conduct impact assessments.
Consent	Consent must be unambiguous and may require opt-in from individuals.	• May need to assess and update consent mechanisms across a wide variety of communication channels.
Right to erasure	Requires organisations that own personal data to erase data relating to an individual and to stop further dissemination of such data, upon receipt of a request.	• Significant effort required to locate and delete personal data. • Issues with partial or incompatible data sets. • Practical difficulties with information processed by third parties.

Understanding the business imperatives

In the following section we highlight four key areas of focus for consumer-facing businesses in developing their cyber strategy.

1 – Develop an integrated approach to cyber security with board-level accountability

Imperative

Cyber threats are increasingly malicious and can have an impact on multiple business functions, cause reputational damage and erode consumer trust. Boards are becoming more aware of the issue of cyber risk but do not 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 compliance with new UK Corporate Governance Code reporting requirements.

The implementation of integrated cyber-risk governance will ensure that the board is better informed of the potential impact of cyber attack and has direct oversight of risk management processes and budgets to mitigate this risk. The board will thus take informed business and strategy decisions, be more confident in the real level of organisational risk and be able to comply with the new UK Corporate Governance Code if applicable to their business.

Activities

Greater cyber-risk governance is required to enable business driven decision-making and risk management across all business units including IT and information security, and to ensure that the board is properly informed and engaged. Organisations need to:

- establish board level responsibility for cyber risk and make cyber security an enterprise-wide issue
- assess and benchmark current cyber-risk maturity, review existing cyber-risk governance, identify primary business impact of a cyber attack and review security regime management and capabilities
- design appropriate cyber-risk governance structure and processes in the context of the corporate governance model, risk culture, business sector, and potential business impact
- implement the new governance model including new processes, terms of reference, reporting dashboards and necessary culture change.

Cyber-governance maturity

2 – Know your cyber assets

Imperative

Consumer businesses need to focus on their data assets, and critical IT-enabled processes in order to understand where they are, the controls that are in place and the risks associated to protect brand equity. The challenge is not fundamentally different to physical security on tangible assets: the business cannot protect what it does not know about.

A well-defined governance policy and a clear understanding of the impact of a breach will drive business engagement and enable risk-based governance over cyber-improvement plans.

Activities

- establish governance and ownership of all data, both business and consumer
- perform a data mapping exercise to understand the data held within the organisation including the volume and complexity of information held, where it is stored and which processes depend on it. This includes sensitive consumer and employee information, such as payment card information and bank account data, and other data that makes it possible to identify individual consumers
- identify breach scenarios, and define the likely impact to the business of these crystallising, to enable the business to prioritise risks for mitigation.

3 – Build trust with consumers

Imperative

There is value in the sharing of data for both businesses and consumers. Trust is built by protecting consumers' data, explaining clearly the benefits to them and providing them with choices about how their data is used. While consumers want more protection and will always state that they would like more security, their main focus tends to be on obtaining the information they need for completing the shopping journey in the most seamless and convenient way.

Given the increasing pressure on prices and margins for businesses in the consumer sector, consumers need to be offered more than just a price differentiator; consumer businesses need to demonstrate value. Personalisation of the consumer experience provides additional value, and to do this organisations need to be explicit in how the data is enabling this personalisation and make the benefits clear from the outset. Failure to do this will cause consumers to default back to price as the differentiator, causing increasing margin pressure.

Activities

- provide transparency to the consumer on what data is held
- be clear about the benefits to the consumer, using examples which illustrate how the business will use their data
- give the consumer choice in how their data is used
- implement adaptive authentication and/or single sign-on solutions to improve the consumer journey
- integrate cyber security as part of a brand protection strategy using threat intelligence to monitor and take down fake websites.

4 – Develop a response plan

Imperative

Businesses in the consumer sector all need to be able to prevent cyber-security incidents. It is no longer a question of 'if' but 'when' they will suffer a breach. Therefore organisations need to have the capabilities in place to detect and respond to an incident in a controlled and planned manner.

It is critical for organisations to have a plan for how they will respond and ultimately recover from a security breach. In 2015 there have been numerous examples of security breaches significantly damaging a business almost overnight. Response and recovery are key to reducing the impact of the breach on the organisation and limiting the damage. Organisations who have a prepared response and communication plan, and who are proactive in engaging affected customers, have seen less of a long-term impact on their trading and share price.

Activities

- develop an incident response plan which integrates all parts of the organisation, up to, and including, the board
- perform planned and unplanned exercises to test the incident response plan
- have a clear communications plan for a cyber incident, including a media response, the way the breach will be managed with consumers to mitigate the reputational risk
- gather intelligence about types of attacks and monitoring to ensure that suspicious activities are detected and investigated
- develop capabilities to perform forensic investigations, and ensure that lessons are learned from them.

Endnotes

1. ISTR20, Internet Security Threat Report, Symantec, Volume 20, April 2015.
2. http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html
3. http://www.bbc.co.uk/news/technology-32958765
4. The Deloitte Consumer Review, Made-to-order: The rise of mass personalisation, July 2015.
5. 2015 Global Megatrends in Cybersecurity, Ponemon Institute, February 2015.
6. http://www.information-age.com/technology/security/123459707/britain-paying-price-cybercrime#sthash.bXofjt1B.dpuf
7. http://www.csoonline.com/article/2137120/malware-cybercrime/cybercrime-siphons--3-billion-in-e-commerce-revenue.html
8. http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf
9. http://www.google.com/transparencyreport/safebrowsing/?hl=en
10. http://www.thedrum.com/news/2014/04/28/london-police-ip-crime-unit-suspends-25k-fraudulent-websites-suspected-generating

Contacts

Consumer Business Leadership team

Nigel Wixcey
Partner, Consumer Business Industry Leader
+44 (0)20 7303 5007
nigelwixcey@deloitte.co.uk

Ian Geddes
Partner, Retail Lead
+44 (0)20 303 6519
igeddes@deloitte.co.uk

Graham Pickett
Partner, Travel, Hospitality & Leisure Lead
+44 (0)1293 761232
gcpickett@deloitte.co.uk

Neil Jones
Partner, Consumer Business
+44 (0)121 695 5149
neijones@deloitte.co.uk

Authors

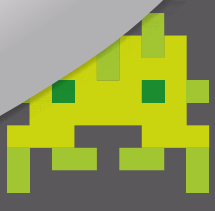
Céline Fenech
Research Manager, Consumer Business
+44 (0)20 7303 2064
cfenech@deloitte.co.uk

Lisa Hamilton
Manager, Cyber Risk Services
+44 (0)20 7007 9619
lhamilton@deloitte.co.uk

Simon Borwick
Director, Consumer Business, Cyber Risk Services
+44 (0)20 7303 6421
sborwick@deloitte.co.uk

Ben Perkins
Head of Research, Consumer Business
+44 (0)20 7307 2207
beperkins@deloitte.co.uk

Contributors: Harvey Lewis and Richie Evans



Designed and produced by The Creative Studio at Deloitte, London. J2887