DataHeaven or DataGeddon?

shaping tomorrow with you

» Having your personal data stolen is like being mugged for your handbag. Nowadays we keep as much information in our online wallet as we do in our purse. So it's no surprise that consumers are beginning to wake up to the dangers that lax security can mean online. As our results show there is a desire for transparency and a real need to showcase the benefits of data-capture to the average shopper.«

David Robinson, CSO UK&I Head of Security Bid and Pre-Sales, Fujitsu

Contents

Introduction

Data is rapidly becoming one of the defining themes of this decade. It is also becoming one of the most divisive.

The origins of the word itself can be found in the Latin word *dare*, literally "something given". Like many words, data's modern application has seen much change since its origin. But there is a certain irony that what began as a given is now, for many, something they would much prefer to be hidden.

Data is no longer the exclusive territory of analysts and scientists. The information we create and leave behind is now the stuff of headlines and documentaries. Data is rapidly taking its place in the national conscious.

Our obsession with data is such that the issue has even bridged over to the silver screen. At the time of writing, cinemas nationwide are showing 2013's *second* film to cover the story of Julian Assange's WikiLeaks. Data is now as good for mainstream entertainment as it is for predictive analytics.

While the frenzy around data may be particularly pronounced at the moment however, our fervour for it is not a new phenomenon. Our relationship with the data we create has always been fragile, and that fragility has only increased in the digital era.

Part of the issue relates to the ever-expanding volume of data.

Google's Eric Schmidt made headlines in 2010 with his assertion[i] that humanity now creates more information in a two-day period than it did in the entirety of the two millennia before. An EMC sponsored study from the following year found that we would need a mountain of iPads 25 times taller than Mount Fuji in order to store the 1.8 zettabytes of information generated in 2011[ii].

Those data mountains are made from the tiniest pieces of gravel. From social media to the Internet of Things, we generate data points at almost every moment of our waking lives. Even previously innocuous activities – from swiping a railcard to changing a TV channel – create a digital footprint that can be used to analyse, predict and even act upon our behaviour.

While we may be conscious of how we share *some* of that information, what about those smaller, less visible data points? How is it used? And do we trust those organisations that hold it to secure and manage it?

Those issues form the basis for this report. Our research was founded on the desire to explore two key themes:

- Our trust in the ability of the organisations we deal with day-to-day to manage our information securely
- And the (largely invisible) contract that exists between the consumer and the organisation – the idea that as the amount of data those organisations hold on us grows, so too should their ability to provide a more enhanced personalised service.

Few subjects elicit such an emotional response as our personal information. Additionally, the definitions of 'good' and 'bad' in this area are intensely fluid.

If the consumer's view is that they are being spied upon, for instance, the insurance company's view may be that they are limiting their own risk exposure and thus doing 'good' for their shareholders. There are few, if any, right or wrong answers.

At the same time, we wanted to provide readers of this report with enough insights to draw their own conclusions on the data dilemma – where brands are struggling or succeeding, and where there is clear, compelling evidence of room for improvement.

There are many things to be optimistic about. When data is used in the right way, it can enhance loyalty, engagement, spending – and everything in between. But it is also clear there are some fundamental obstacles that need to be overcome first.

The challenge for organisations of all kinds is in finding their path to a "data-heaven" – not just for them, but their customers too.

Executive summary

Trust in organisations to hold our data

Across the board there is little trust in organisations to securely hold our data. Nearly a third of respondents (29%), confirmed their trust in organisations ability to keep information secure had declined over the last year. Why? A huge 69% said it was down to a lack of trust in organisations.

Only 9%

of respondents believe companies are doing enough to secure their data.

Which sectors are thriving and which are struggling?

Every single sector has seen a drop in trust over the last 10 years, however, based on implicit trust it is the financial services sector that has seen the biggest decrease, with a 16% drop. While over half of respondents had trust in their banks 10 years ago (52%), now only just over a third do (36%). Despite this, it is still the most trusted sector overall.

It is social networks which consumers have the least trust in.

Today, only 15% of consumers say they trust the sector with data. Coming just above this were telecoms/media, utilities and local government – who all have a trust level of less than a quarter (24%).

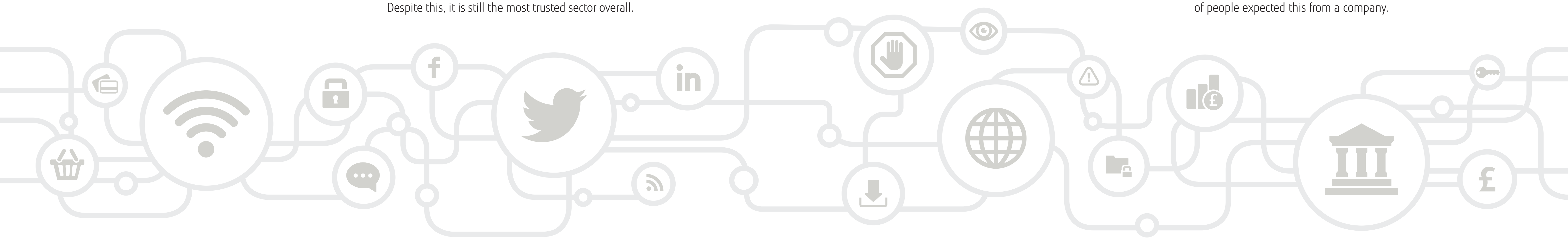
Where does the buck stop?

Over 4 in 10 respondents (43%) felt that individual organisations were responsible for the data they hold; over a quarter of respondents (27%) felt the Government was responsible. However, when it comes to action being taken post-data breach, we want an individual held accountable and dealt with – a third of people expected this from a company.

Despite this, consumers also recognise their own involvement in keeping data secure –

68%

said they held themselves responsible.



A decade of decline

Trust and the modern consumer

Do we trust the organisations we deal with on a daily basis to safeguard our information, to use it in the 'right' way? Do we fully comprehend or care about what data those organisations might hold on us?

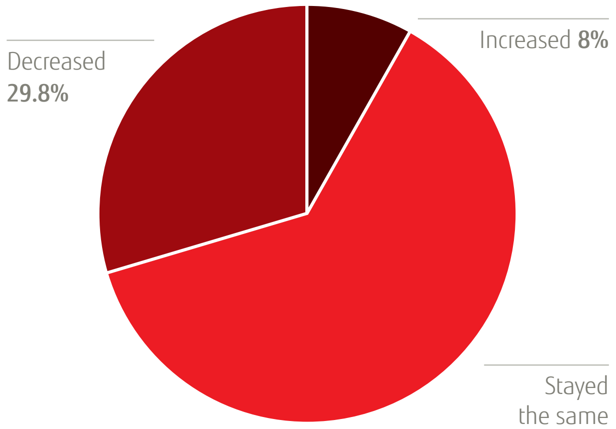
Our investigation into the current data views of UK consumers began with a specific look at how their perceptions might have changed over the past year.

Asking our respondents to tell us whether their trust in the ability of organisations to keep your personal information secure had changed in the past 12 months:

- **62%** said that their level of trust remained **unchanged**
- **30%** said that it had **decreased**
- And just **8%** said that they trust organisations with their data more today than they did a year ago

Fig 1

Over the last 12 months, how has your trust changed in the ability of organisations to keep your personal information secure?

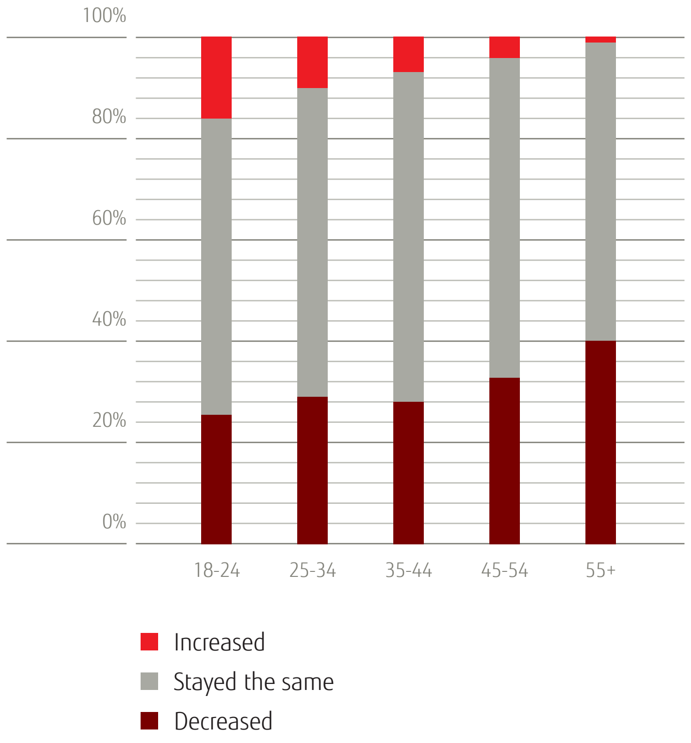


This erosion of trust appears to be felt most acutely by the older generation. Those aged 55 and above were much more likely (40%) to suggest they were less trusting of organisations to safeguard their information. Just 1% of this group say that their faith in those parties has increased.

Conversely, teenagers and those in their early 20s are the most likely to be reassured that their data is in safe hands. 18-24 year-olds are twice as likely (16%) to say that their confidence in organisations to protect their privacy has increased, and are less likely than any other group (24%) to say that it has decreased.

Fig 2

Variations in trust by age group



Is this an issue of technophobia? Our personal data is commonly linked with the digital services, applications and social platforms we use, putting it in the heartland of the (perceived-to-be) tech-savvy young.

Does the older mindset lead to a more cynical attitude towards data privacy and security in an era of "always-on" technology? To find out, we asked those who expressed that their level of trust had diminished to tell us why.

"Trust" as a whole was a major issue. 65% noted that they had concerns about whether the Government would use their data securely, matched closely by 69% who said the same of any organisation that holds their data.

Media coverage of issues relating to data security and privacy also seems to be responsible for dwindling trust. 21% noted that Edward Snowden's revelations around the USA's National Security Agency PRISM programme – allowing it to tap into consumer communications on and offline – had influenced their thinking, with 19% noting that they had seen an incident of personal data theft or loss reported on in the news.

These factors combined seem to point to an overall heightened awareness of security, with 48% noting that they are generally more conscious of data issues.

Fig 3

If your trust in organisations to safeguard your information has decreased over the past year, why would you say this is?

Choice	%
I have less trust in the Government to use my data securely	65%
I have less trust in the organisations that hold my data	69%
The PRISM scandal	21%
Influence of your family/friends	4%
A personal experience of my information being lost/stolen	13%
An incident of personal information being stolen/lost that I saw on the news	19%
I am more aware of the issue generally	48%
I don't know	4%

While responses to this line of questioning tracked broadly the same across all age groups, some standout statistics tell a story of their own. Older respondents (55+) are far less likely to trust organisations with their data, with 83% of this group voicing their concerns. They also report that they are more aware of data security than average, at 62%.

Rolling back the years: data confidence in 2003

Although the 12-month view on data security is a useful snapshot into why we feel the way we do today, to truly understand the issue we wanted to look even further back.

Establishing a trust score

Across eight major vertical markets, we asked consumers to tell us how they felt they trusted organisations to protect their data today, a year ago, five years ago and – finally – a decade ago.

Respondents were asked to give an answer on a scale of one to five (where one is 'no trust' and five is 'trust implicitly') for all of those time points.

From this, an average score was produced for each moment in time.

We'll explore each of those verticals in more detail below, but some key themes very quickly arose when analysing the responses to this question.

- **The erosion of trust has been slow but steady:**
  Every sector we investigated has seen a decline in consumer trust on data management since 2003. While this erosion of trust has been more dramatic in some sectors than others, each has seen a notable drop in confidence over the past decade.
- **Banks and other financial institutions have suffered worst, but we still trust them more than most:**
  Perhaps a consequence of what has been a difficult decade for financial institutions generally, banks and insurance companies have seen the greatest drop in trust over the past 10 years. It is notable however, that these companies led the way in 2003, our trust in their ability to safely manage our data higher than any other sector at that time – and the same remains true today.
- **Our view of social networks and search engines has always been dim:**
  Indicative of our sometimes 'confused' relationship with social networks and search engines (we love to share our information and depend upon search, but worry about who sees the results), consumers have rarely placed much trust in these channels to look after our information sensitively. Social networks scored lowest of all in the 'high trust' rankings – though that score has remained largely stable since 2003.
- **Retailers, both online and off, seem to have earned our trust:**
  As with every other sector, trust in high street and internet retailers to safeguard our information has dropped – but comparatively little when compared to other parties. We'll consider why that may be later in this report.
- **Confidence in government has fallen steeply:**
  Government organisations and agencies – both central and local – have suffered in equal measure. Consumer confidence in central government to manage data securely took the second steepest drop seen in this study.

Banking and insurance

Financial institutions have dropped from an average trust score of 3.52 in 2003 to 3.07 today. The most notable change here has been the number of people saying that they implicitly trust these companies to look after their data, dropping from a perceived 21% a decade ago today to just 11% today. Those saying that they have 'no trust' in this sector has doubled correspondingly – up from 6% in 2003 to 13% now.

High-street retail, supermarkets and hospitality organisations

While high-street retail may be another sector to suffer a difficult 10 years, our confidence in bricks-and-mortar stores to look after our data has remained relatively undiminished. An average score of 3.27 in 2003 has given way to one of 2.95 today. While this may not be cause for concern itself, the rise in the number of people saying they have 'no trust' for these businesses in the past five years has been acute – from 4.8% in 2008 to 11.3% now.

Online retailers

eCommerce has evolved considerably from the early days of the internet. Widespread concern about the potential for rogue trading has given way to a huge number of legitimate, international businesses. Overall – and perhaps surprisingly given the timespan – online retail tracks almost identically to its high-street counterpart. An overall trust score of 3.20 from 2003 now stands at 2.94. With 6.5% of respondents citing implicit trust in online retailers, this group now holds second place in the confidence league table.

Telecoms or media companies

Consumer trust in these organisations has never been particularly high. Recalling their feelings from 2003, only 8.8% said that they were 'highly' trusting of telecoms and media companies in relation to personal data. With an aggregate data trust score of 3.09 in 2003 dropping to 2.79 today however, the decline in confidence for this group has been relatively small when compared with others.

Utility companies

Utilities occupy the middle ground of the consumer psyche when it comes to data privacy and security. Unlikely to be seen as implicitly trustworthy either in 2003 (11%) or today (6%), neither are they particular cause for concern; 14% stress that they have 'no trust' in utilities to manage their data securely today, placing these businesses squarely alongside the overall average when social networks are removed from the equation. Overall data security trust here has dropped from an average of 3.18 points in 2003 to 2.84 today.

Central government

Some of the 21% of respondents who noted that the PRISM scandal had diminished their confidence in organisations to safeguard their personal data may be found in the scoring for central government. Central government organisations have suffered the second-steepest drop in confidence after financial institutions – down from an average score of 3.18 to 2.79 over the past decade. Most alarming will be the drop in those with 'high trust' in 2003 (14.4%), standing at just 6.3% today.

Local government

Regional and local government organisations have not escaped the fate of their centralised colleagues. Trust in their ability to manage our data has fallen from an average of 3.14 points to 2.77, with 16.9% now saying they have no faith at all in local government in this area (the second highest 'zero confidence' result in the study). Just 5.7% of people say that they have full trust in councils and other local government institutions to manage our data securely and privately.

Social networks and internet corporations

And so on to the standout group within this report. Social networks and internet corporations track considerably lower than any other organisation over issues of data privacy. At 31.1%, social networks stand at almost double the nearest 'no trust' response from consumers. They are cursed with the lowest overall trust score (2.35 points) today, with even their decade-ago high of 2.57 failing to match even the lowest current scores from any other group.

> One point of hope would be that – in spite of the PRISM saga – those with 'high trust' for this group has actually increased in the past 12 months, stable at 4.3% one year ago to
>
> **4.5%** today.

The invisible contract

Trading personal information for a better experience

Trusting organisations to keep our data safe is not the same as trusting them to use it in what we consider to be the 'right' way.

Marketers and customer service professionals alike extol the virtues of being able to create deeper, richer and more personalised customer experiences via greater insight. But do consumers care? Do they see that experience in action? Moreover, do they even feel comfortable with that level of personalisation?

To expand on that issue, we began by asking two broad questions relating to that 'invisible contract' – the trade we make between our personal information and (what should be) a more tailored experience. The results were telling.

Firstly, we asked consumers to consider whether they cared which organisations and Government bodies stored their personal data. 81% said that they did (with a more surprising 19% revealing an apparently laissez-faire attitude to information ownership).

Secondly, we asked them to tell us outright whether they felt that any organisation they deal with on a daily basis (for instance banks, shops or utility companies) should use personal information about them to improve their experience of dealing with them. A resounding 63% said that these organisations should not.

Should this spell the end for customer loyalty schemes? Would personalised marketing emails be better off consigned to the 'drafts' folder? Perhaps not. As we will come to see, the challenge for brands from all sectors is to prove to that 63% that they can do two key things:

- Collect, manage and store consumer data securely
- And conclusively prove the benefits of a more personalised service

Data in action, or data inaction?

As with any customer experience, proof is a great confidence builder.

Just as shoppers will choose brands based on past experiences of quality or value, one of the major challenges for organisations seems to be in proving that they can deliver on the data dream – that they can offer a personalised experience that consumers care about.

Our research suggests that this is easier said than done. Once again, respondents were asked to rate our chosen sectors on a scale of one to five, we asked consumers to tell us the degree to which they feel their information is currently being used to provide a better experience. A score of five was used to represent a 'very high' standard of service, with one representing a 'very low' standard.

Results were, at best, middling:

- **Retail leads the charge, but fails to break away:**
  Only retailers come close to offering a better quality of service through the application of customer data, with both online and high-street retail scoring an average 2.93.
- **Financial institutions place second:**
  With an average score of 2.75, banks and insurance companies are chasing retailers for first place in the customer experience table. With 7.3% of consumers noting that they offer a 'very high' standard of personalised service, these companies seem to be catching up fast.
- **Most other organisations struggle to get above average with an improved service:**
  Below the leading pack of retail and financial services, most other sectors struggle. Scores range from slightly below average (local government at 2.4) to slightly above (telecoms and internet corporations at 2.6), with most consumers seemingly uninspired by the standard of service they receive.

Results show significant room for improvement.
If consumers are concerned about which companies hold their data and unconvinced that it should even be used, they are given too little proof that their information can be used to offer them a better service.

The trade: be secure and take my data

Is security the defining factor in how customers authorise use of their personal data? 96% of those surveyed either 'somewhat' or 'strongly' felt that the security of their personal information is more important than it being used to offer a better experience.

Digging deeper into why trust has declined over the past decade, we looked to our consumers to expand on their disillusionment – and quickly revealed some major issues.

More than 90% feel that companies are not doing enough to protect consumer information, with more than a third (34%) feeling strongly about this. A similar 89% say they would rather that companies did not store information on them, as they do not trust them to store it safely. 95% say that if their personal information was lost, it would destroy their trust for that organisation forever.

Vitally though, lack of trust is not the endpoint for companies in organisations; it is the gateway to a bigger opportunity. While we see significant misgivings about whether or not companies can store data safely, half of the consumers we spoke to also revealed that they would happily share all of their personal information if it meant they never had to receive irrelevant marketing again.

The message is clear: consumers will trade their data for a personalised service, but only if their security concerns are addressed first.

Fig 4

To what extent do you agree with the following statements?

Choice	Rating	%
The security of my information is more important than how it is used to offer me a better experience	Completely agree	55.57%
	Somewhat agree	40.7%
	Do not agree at all	3.73%
The loss of my personal information would impact my trust of a brand irrevocably	Completely agree	56.83%
	Somewhat agree	39.5%
	Do not agree at all	3.67%
I do not think companies are doing enough to ensure consumer information is secure	Completely agree	34.23%
	Somewhat agree	57.17%
	Do not agree at all	8.6%
I would rather organisations do not store personal info about me because I do not trust them to keep it safe	Completely agree	36.03%
	Somewhat agree	53.87%
	Do not agree at all	10.1%
I will happily share all my personal information if it means I never have to receive irrelevant marketing	Completely agree	9.73%
	Somewhat agree	40.8%
	Do not agree at all	49.47%
I do not think the UK government is doing enough to ensure consumer information is secured adequately	Completely agree	32.77%
	Somewhat agree	57.73%
	Do not agree at all	9.5%

Overall, consumers seem to catch only fleeting glimpses of the data dream. While they are able to single out those organisations that do capitalise on the data/personalisation opportunity, much still needs to be done to convince them of the benefits.

Taking it to the top

Where does the buck stop during a data disaster?
We know already that consumer confidence in organisations of all kinds to manage their data has dwindled over the past decade. But who do they blame when things go critically wrong?

With the Information Commissioner's Office now handling in excess of 13,000 cases a year regarding Data Protection[iii], we wanted to uncover the lengths that today's consumer will go to if they feel their data has been lost or misused.

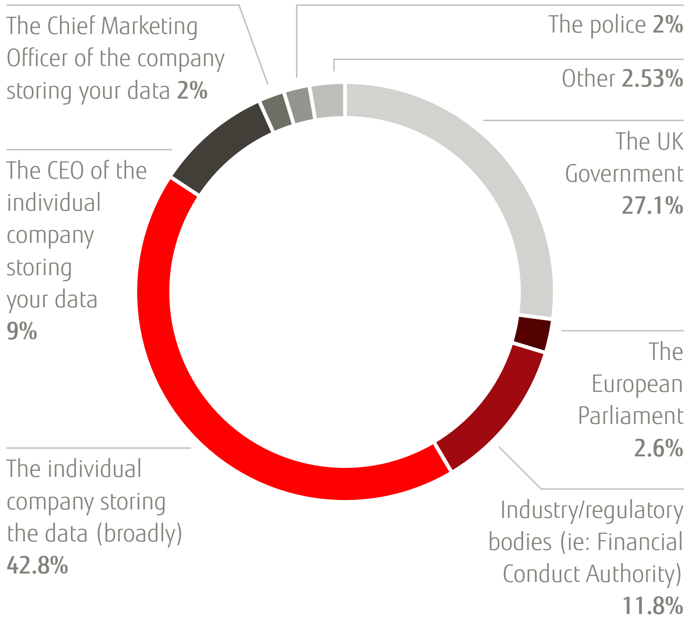
To start exploring that issue, we asked study respondents to explain who they felt was ultimately responsible for ensuring the security of information stored about them. They were allowed one choice only.

While some pinned the ultimate responsibility on the Government (27%) or industry bodies, the majority (43%) suggested that they held individual companies to account when it comes to the security of their data.

One response here that may make for uncomfortable reading around the boardroom table is the suggestion that almost 1-in-10 (9%) now hold the CEO personally accountable for data breaches or misuse.

Fig 5

Who do you think is ultimately responsible for ensuring information stored about you is secure?



Following on from that question, we wanted to investigate what specific actions our group would take if their data was lost by a business. Respondents were asked to select any that apply, with some particular points of interesting arising:

- **One in five say they will treat it as a criminal offence:** A staggering 20% suggest that they are prepared to contact the police if a company loses their information. This becomes even more surprising when we consider that this matches exactly the percentage that say they will express their discontent on social media channels. Over 55s are more likely than average to make data loss a police issue – 31% saying that they would contact law enforcement over a breach.
- **More than half would stop using the company in question:** 51% suggest that data loss is now a serious enough issue to warrant taking their custom elsewhere. Particularly relevant to banks, insurance companies, retailers, telecoms, media, social networks and internet corporations, this was the most common response cited by our panel. 44% would steer their friends and family away from the business as well.
- **One third want to make it personal:** With some people suggesting that they see the CEO or CMO holding responsibility for the safety of their data, it follows that many also want to see individuals held accountable. 33% said they will seek assurances from a company that the person or people responsible for losing the data had been held accountable. 43% would want to see improvements in security, with 32% seeking compensation.

Fig 6

What actions would you take if a company lost your personal information?

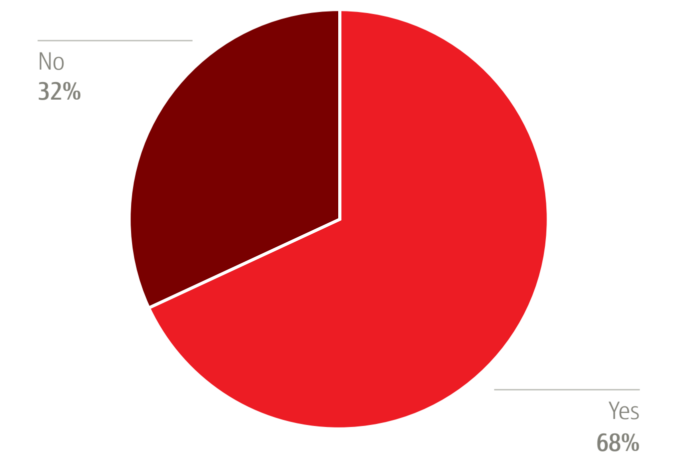
Choice	%
I would be concerned but not take further action	13.9%
I would seek assurances from the company that they have increased security	42.5%
I would seek assurances from the company that the person/people responsible had been held accountable	33.2%
I would report them to the ICO – Information Commissioners Office	29.9%
I would inform the police	20.1%
I would stop using them/move my business elsewhere	51.2%
I would warn my friends/family to the situation and advise them not to use them/work with them	44.1%
I would seek compensation from the company	31.6%
I would voice my complaint / issue on social networks	20.6%
Other	5.1%

Any readers talking to their legal department about personal accountability for data loss can probably afford to rest easy for a little longer.

Although consumers are clear that they will escalate the issue quickly should their data be lost, they are also quick to abdicate responsibility themselves: some 32% of our panel say that the safety of their online data and information isn't an issue they hold themselves accountable for.

Fig 7

Do you believe that you are responsible for the security of your online data and information?



Conclusion

Positivity towards data security seems to have declined almost as steadily as awareness of how it may be used has risen. Consumers are savvy, switched-on and ready to act if the companies and organisations they interact with on a daily basis fail them on data security. The modern citizen demands respect for their data; not only in how it is collected and used, but how it is stored and managed.

These somewhat spiky truths should not be cause for concern. They are blanketed in the clear message that much of our consternation regarding data revolves around security. Opportunities are abundant for those organisations that prove they can be trusted to keep consumer information locked down and accessible only to those who should have it.

The results of our research show three clear imperatives:

1. **The gradual decline in trust must be countered**
The collection, processing and usage of personal data will only increase. This activity cannot run in tandem with a consumer audience that is increasingly disillusioned by it. Organisations of all kinds need to quickly move to the point at which they are offering genuine value and engagement based on the data they hold about their customers, or risk losing those customers forever.

2. **Security comes first, always**
No question we asked relating to personal data generated such a sharp response than the prospect of it being lost by an organisation. Security appears to be the governing factor in the many issues around data privacy and organisations need to rise to meet that challenge. Consumers are demanding over security, but they are also – in the main – fair and reasonable. They have a clear understanding of where responsibility lies and ask only that their data is treated with respect.

3. **Organisations need to focus on proving that they handle data securely**
Simply being secure is no longer enough. Organisations need to actively showcase that they hold their consumer data in the highest regard. Trust does not come as a given and the vast majority of organisations need to work hard to regain some of the ground given up over the past decade.

Those that are able to conclusively show that they offer the highest standards of protection are most likely to make those gains – forging a path towards a DataHeaven, while others skirt perilously close to a DataGeddon.

Methodology

Research for this report was conducted by **OnePoll**, an independent research consultancy based in London. 3,000 consumers from across the UK completed an online survey during October 2013.

A full breakdown of audience demographics can be found in the charts below:

Gender	%	Responses
Female	66.30%	1989
Male	33.70%	1011

Region	%	Responses
East Anglia	5.30%	159
East Midlands	3.57%	107
London	20.63%	619
North East	5.40%	162
North West	11.30%	339
Northern Ireland	1.77%	53
Scotland	8.80%	264
South East	10.53%	316
South West	7.60%	228
Wales	5.43%	163
West Midlands	9.37%	281
Yorkshire and the Humber	10.30%	309

Age Range	%	Responses
18-24	12.23%	367
25-34	32.27%	968
35-44	26.63%	799
45-54	19.70%	591
55+	9.17%	275

Sources and references

[i] **Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003:** Tech Crunch, 4th August 2010

[ii] **How Much Data Will Humans Create & Store This Year?:** Mashable, 28th June 2011

[iii] **Key Facts:** Information Commissioner's Office, as of 11th October 2013

FUJITSU

Fujitsu Technology and Service Vision

The Fujitsu Way

Through our constant pursuit of innovation, the Fujitsu Group aims to contribute to the creation of a networked society that is rewarding and secure, bringing about a prosperous future that fulfils the dreams of people throughout the world.

Read the Fujitsu Technology and Service Vision
fujitsu.com/global/vision/paper

FUJITSU

22 Baker Street
London W1U 3BW

Contact us on:
Tel: +44 (0) 870 242 7998
Email: askfujitsu@uk.fujitsu.com
Web: uk.fujitsu.com
Ref: 3475

Fujitsu Services Ltd endeavours to ensure that the information in this document is correct and fairly stated, but does not accept liability for any errors or omissions.

uk.fujitsu.com