BEYOND THE BOTTOM LINE:

THE REAL COST OF DATA BREACHES

RESEARCH RESULT / MAY 2016

FireEye

RESEARCH METHODOLOGY

FireEye commissioned independent technology market research specialist Vanson Bourne to undertake the research upon which this report is based.

5,500 interviews took place during April 2016 with regular consumers aged 18 or older. Interviews were carried out in five territories, with respondents split as follows: France (1,000), Germany (1,000), United Arab Emirates (UAE) (1,000), Nordics (500) and the U.S. (2,000) with natural fall out across gender and age bands.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

In addition, at the end of 2015, 1,000 U.K. consumers were interviewed with a similar questionnaire, and where relevant, the results to the U.K. study are combined with the 2016 results.

Demographics

1,000 consumers from the U.K. were interviewed in December 2015 and 5,500 consumers from France, Germany, Nordics, UAE and the U.S. were interviewed in April 2016, split in the following ways:

FIGURE D1: Analysis of respondent country, all respondents (6500)

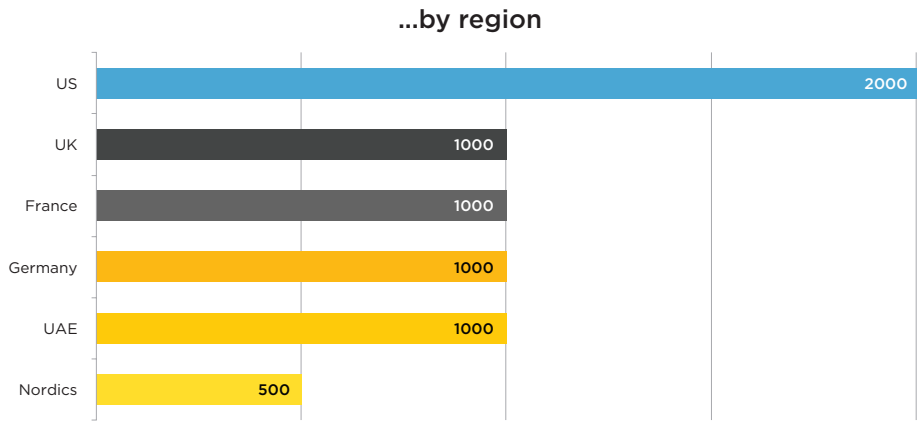


FIGURE D2: "What is your gender?", asked to all respondents (6500)

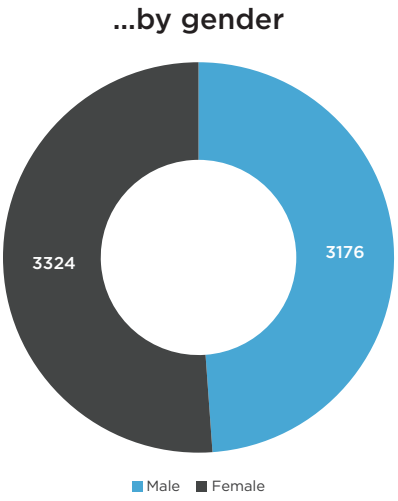
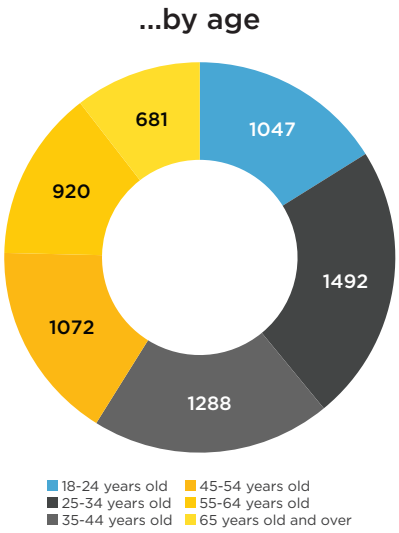


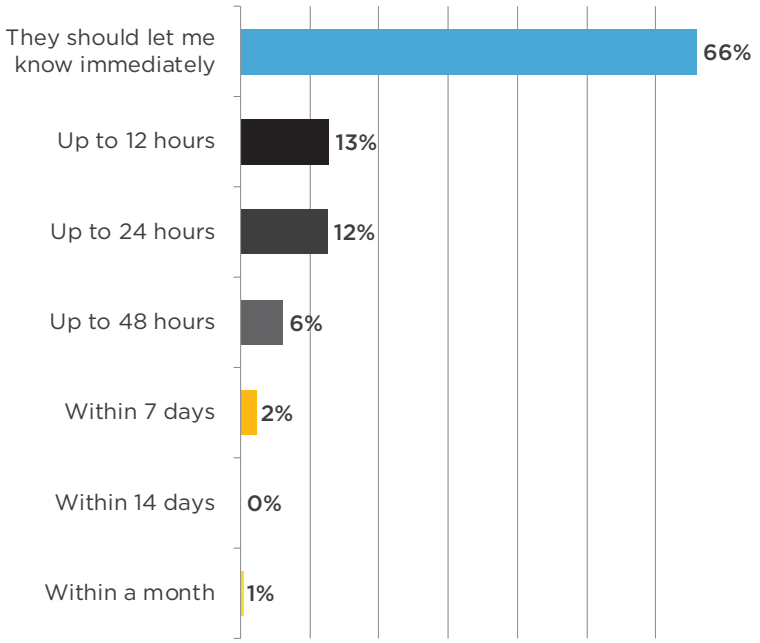
FIGURE D3: "What is your age?", asked to all respondents (6500)



Informing consumers of a data breach

Two thirds (66%) of consumer respondents expect to be informed immediately if a data breach occurs to an organization that holds their data.

FIGURE 1: "What would you deem an acceptable amount of time for an organization that holds your data to let you know that it has been breached and that hackers potentially have obtained your data?", asked to all respondents (6500)

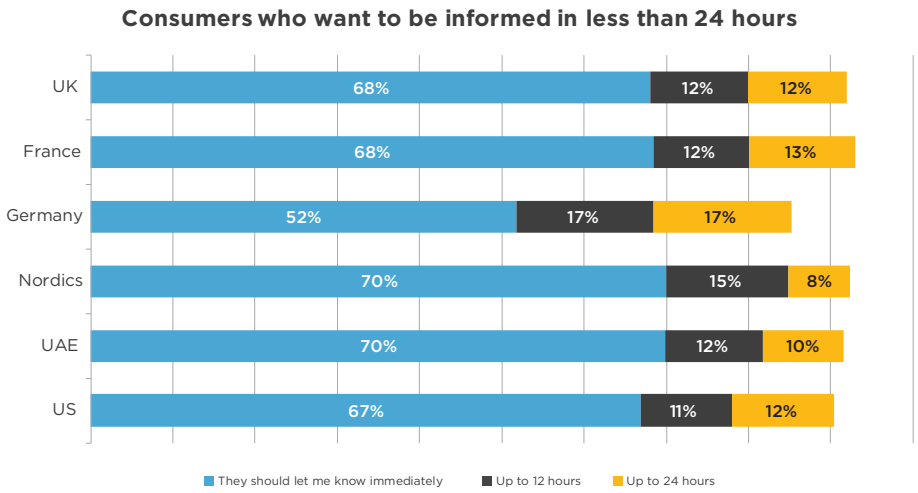


On average, consumer respondents expect to be informed within 13 hours of a data breach occurring. For the vast majority (91%), it should be within 24 hours.

Most consumers find delays unacceptable for organizations to warn them of a data breach, but how aware are consumers of the impact that breaches could have on them?

Regional insight

FIGURE 1A: Regional analysis of consumer respondents that deem 24 hours or less as an acceptable time to be informed of a data breach, all respondents (6500)



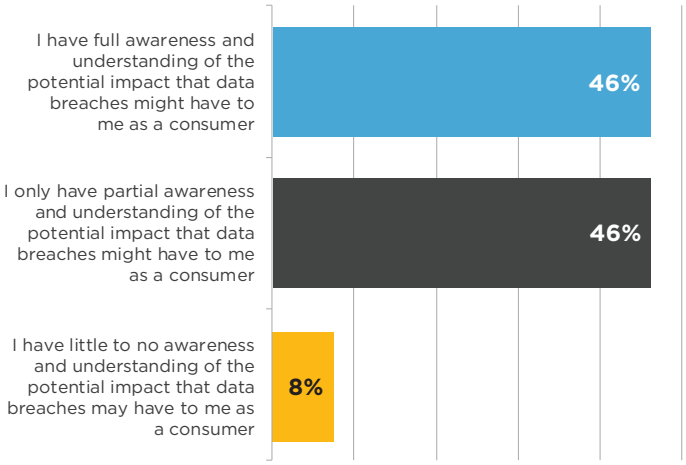
Consumers awareness of how data breaches impact them

Close to half (46%) of consumer respondents report that they have a full awareness and understanding of the potential impact that a data breach can have.

A similar proportion (46%) have a partial awareness with only the minority (8%) of consumer respondents saying they have little to no awareness.

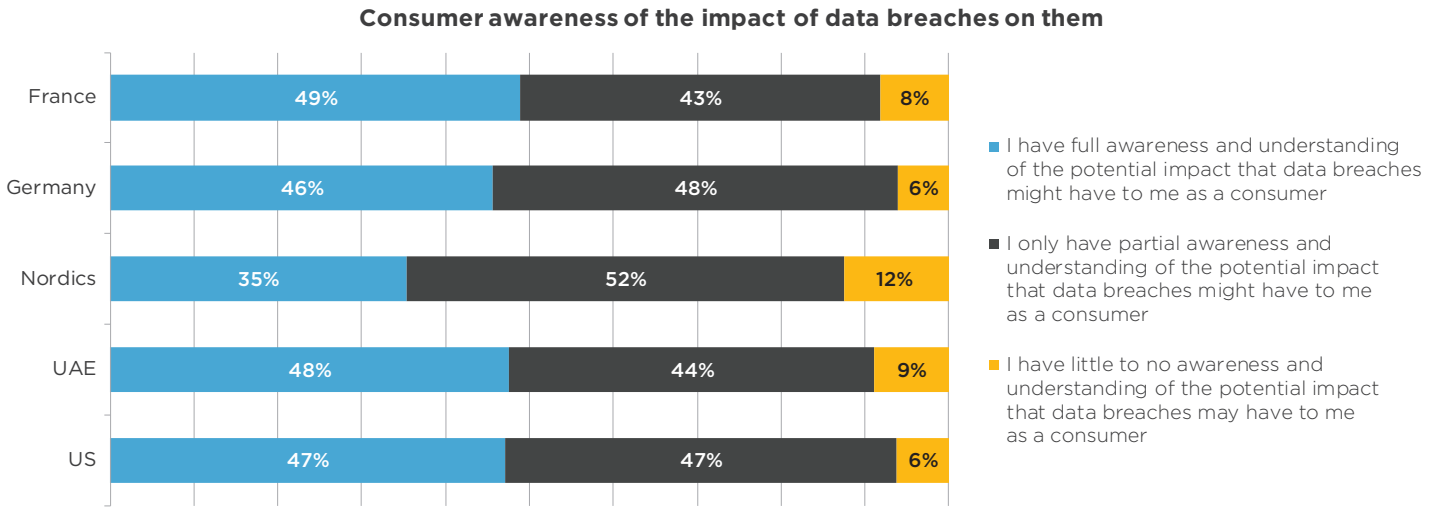
Many consumers have or are developing an understanding on the impact of breaches, so how do they view the security of affected organizations compared to their peers?

FIGURE 2: "How aware are you of the potential impact that a high profile data breach suffered by a company that you use might have on you as a consumer?", asked to all respondents (5500 – not including UK)



Regional insight

FIGURE 2A: Regional analysis of consumer respondents' awareness of the potential impact of data breaches on them as consumers, all respondents (5500 – not including UK)



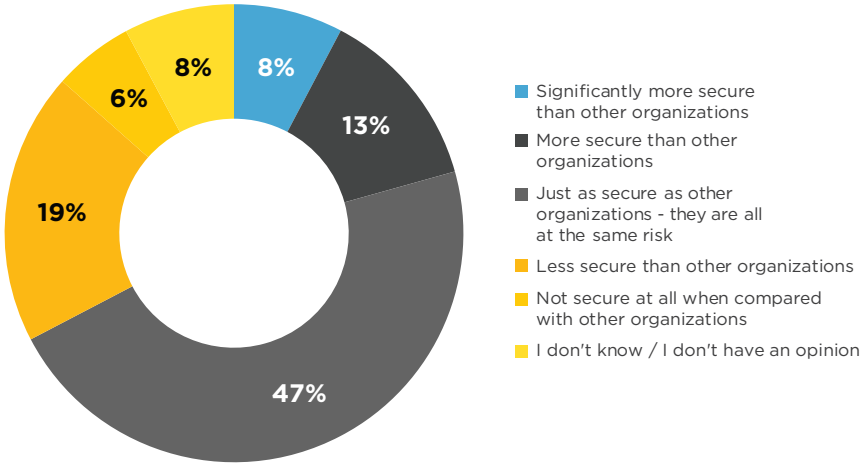
Perceived security of breached organizations

A quarter (25%) of consumer respondents believe that their data would be less secure with an organization that has been breached, or not secure at all, compared to an alternative supplier.

For almost half (47%), all organizations are perceived to be at the same risk and only 21% believe that breached organizations would be more secure to purchase from.

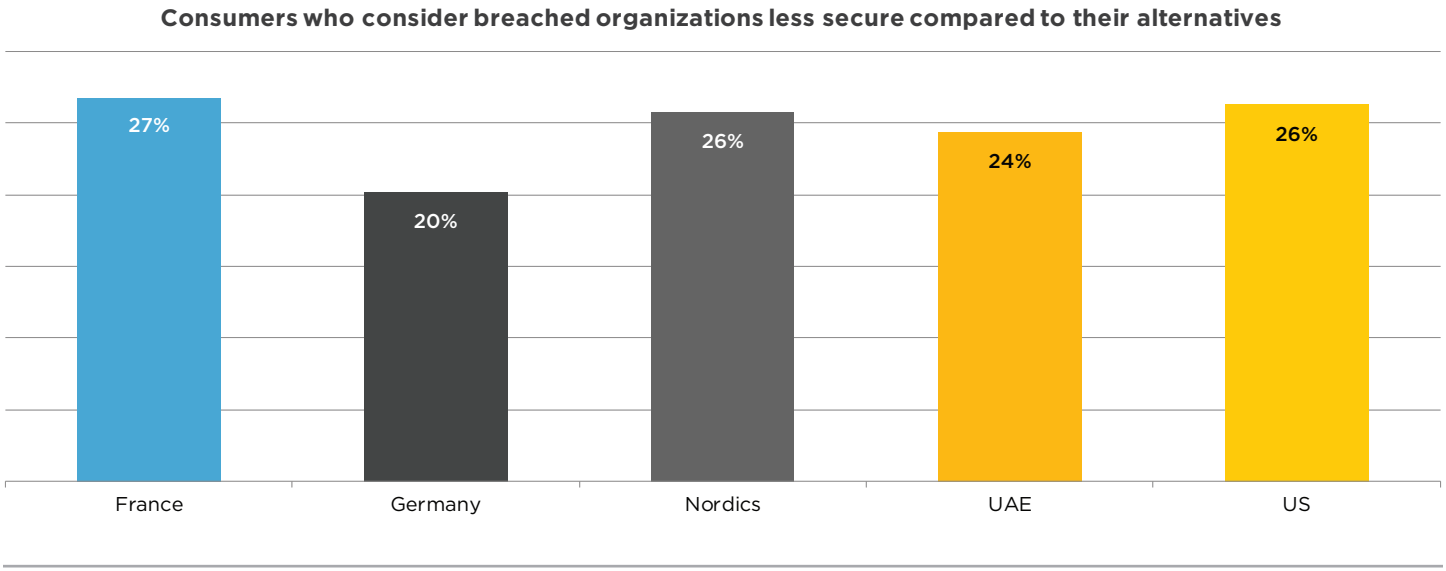
The threat of data breaches is causing many consumers to rethink their opinions of organizations, so how are loyalty and perception impacted by data breaches?

FIGURE 3: "When considering making a purchase from an organization that has been breached, would you consider your data more or less secure with them, when compared to their alternatives?", asked to all respondents (5500 – not including UK)



Regional insight

FIGURE 3A: Regional analysis of consumer respondents' who believe that breached organizations are less secure than their alternatives, all respondents (5500 – not including UK)



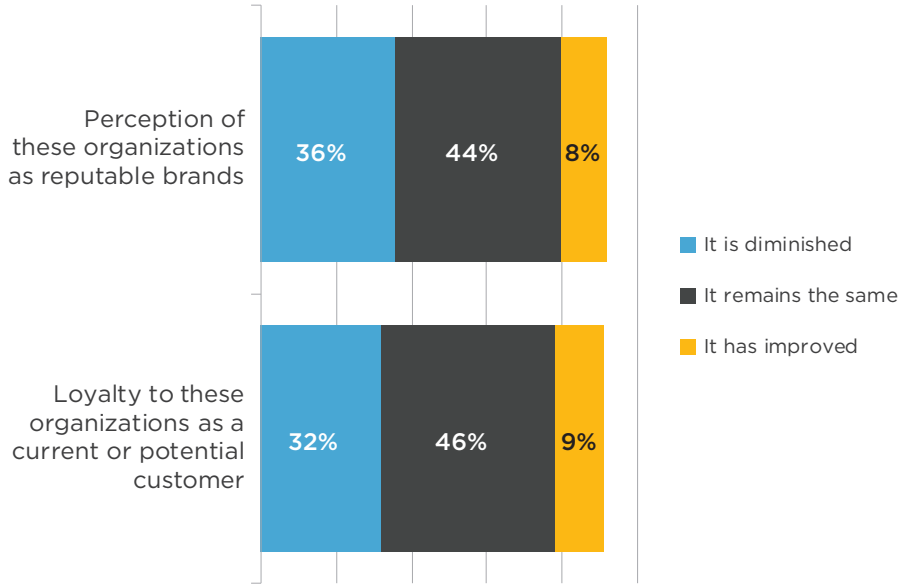
Impact of data breaches on consumer loyalty and perception

Close to four in ten (36%) consumer respondents say that their perception of breached organizations has diminished.

For around a third (32%), their loyalty as a current or potential customer has also diminished as a result of data breaches and the organizations' response.

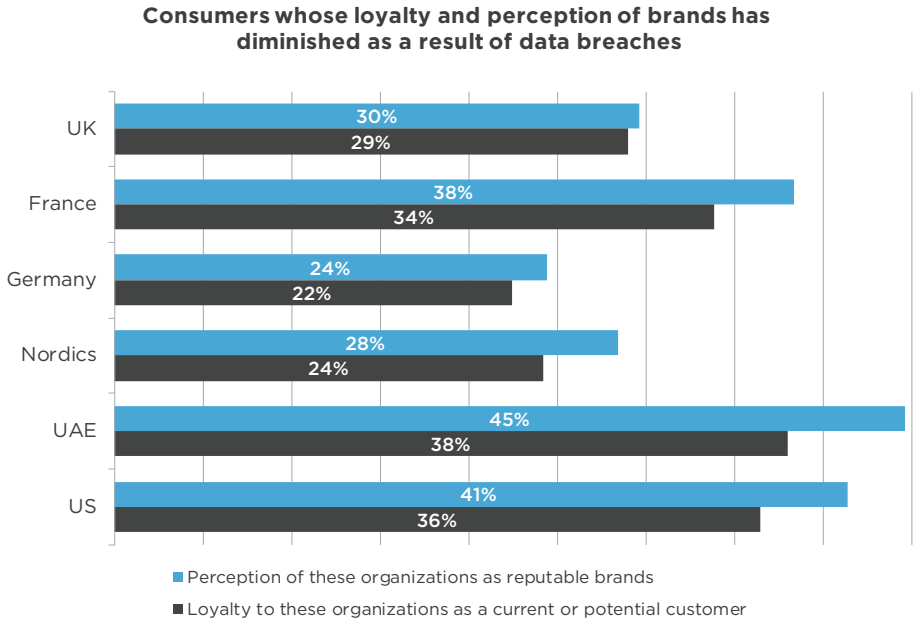
Organizations that have been breached face more than just financial implications, they are at risk of losing customers and facing damage to brand perception. Does the threat remain with just organizations that have been affected?

FIGURE 4: "Have these data breaches and the organizations' responses affected your perception of them as reputable brands and, if you have been or will be a customer, your loyalty to them also?", asked to all respondents (6500)



Regional insight

FIGURE 4A: Regional analysis of consumer respondents' whose perception of and loyalty to breached organizations has diminished, all respondents (6500)



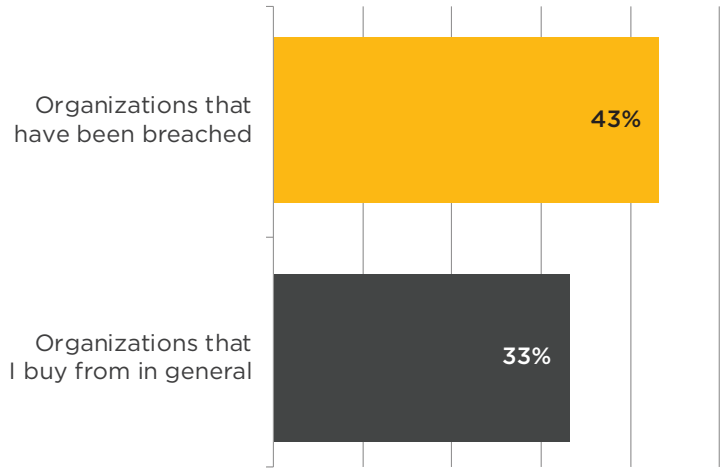
The impact of data breaches beyond just the organizations involved

A third (33%) of consumer respondents now feel more negatively about organizations in general as a result of high profile data breaches.

More than four in ten (43%) feel more negatively about the organizations that have been breached.

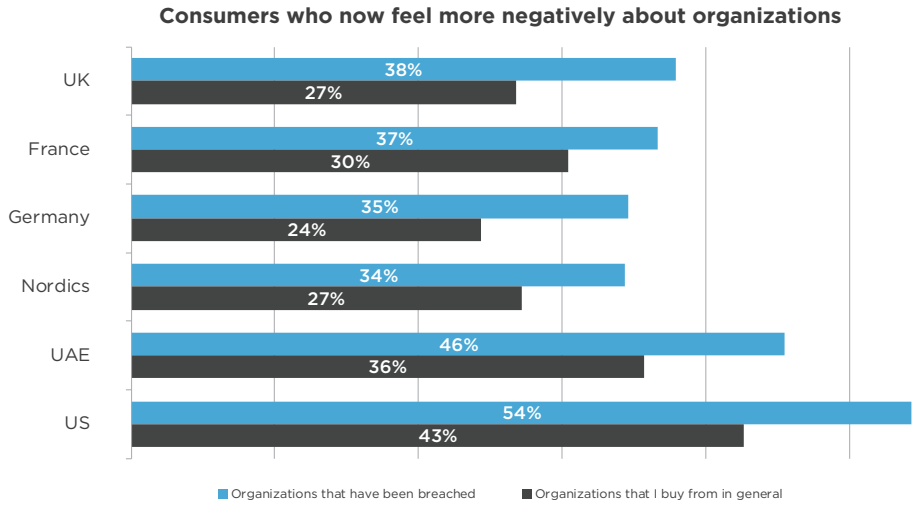
It is clear that recent high profile data breaches are not just impacting upon consumer opinions of the organizations involved, the impact is much wider. What are the specific reasons consumers have for feeling more negatively?

FIGURE 5: Analysis of consumers that now feel more negatively about organizations as a result of high profile data breaches, asked to all respondents (6500)



Regional insight

FIGURE 5A: Regional analysis of consumer respondents that now feel more negatively about organizations as a result of high profile data breaches, all respondents (6500)



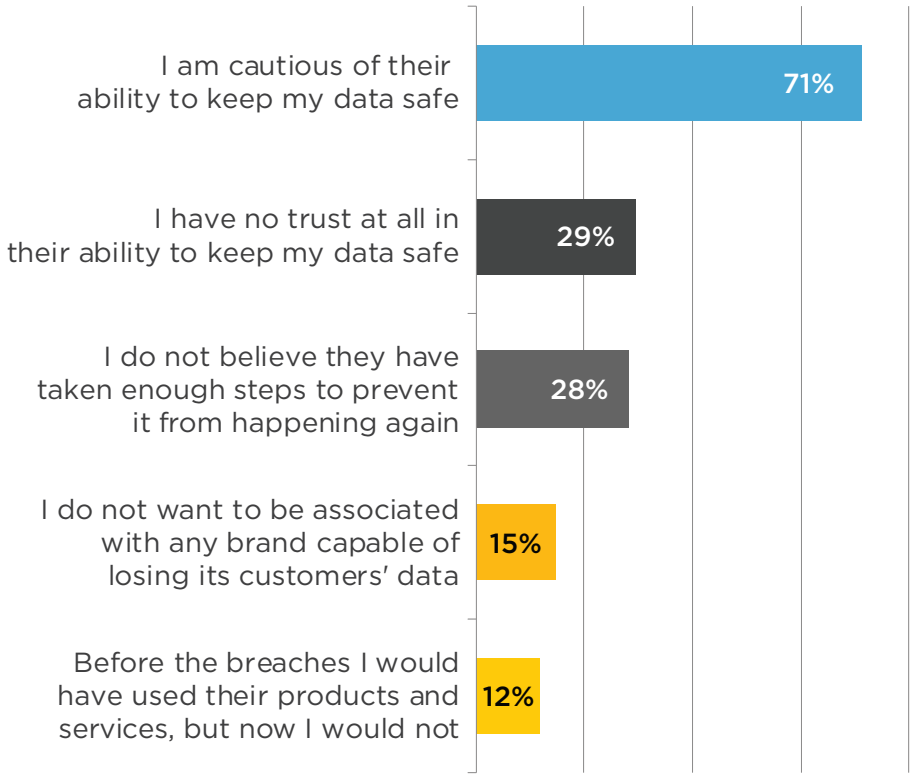
Reasons for consumers' negative perceptions of organizations

Over seven in ten (71%) of consumer respondents who feel more negatively about organizations as a result of data breaches say it is due to concerns about their ability to keep data safe.

Around three in ten consumer respondents report a lack of trust in organizations or that they do not believe enough actions have been taken to prevent a repeat.

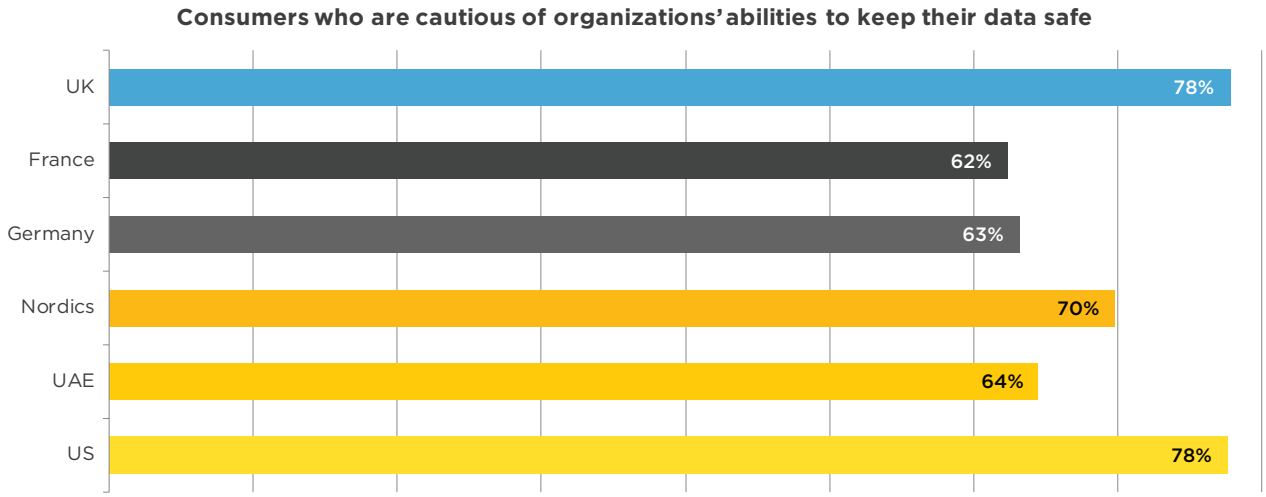
Organizations must rebuild the trust that many consumers have lost in their security capabilities.

FIGURE 6: Analysis of consumers respondents' reasons for feeling more negatively about organizations as a result of high profile data breaches (3161 respondents)



Regional insight

FIGURE 6A: Regional analysis of consumer respondents' who say that they are cautious of organizations' abilities to keep their data safe as a result of high profile data breaches, all respondents (6500)



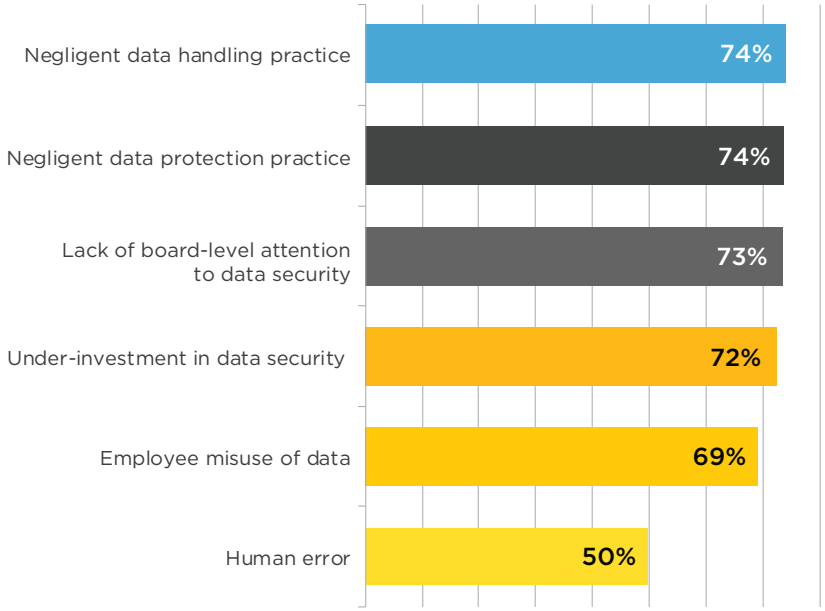
Consumers' reasons to abandon at-fault organizations

Around three quarters (73%) of consumer respondents report that they would be likely to stop purchasing with an organization if they found out that the theft of their data was due to a lack of board-level attention to security.

For a similar number, negligent data handling (74%) and negligent data protection (74%) would also be likely to drive them away.

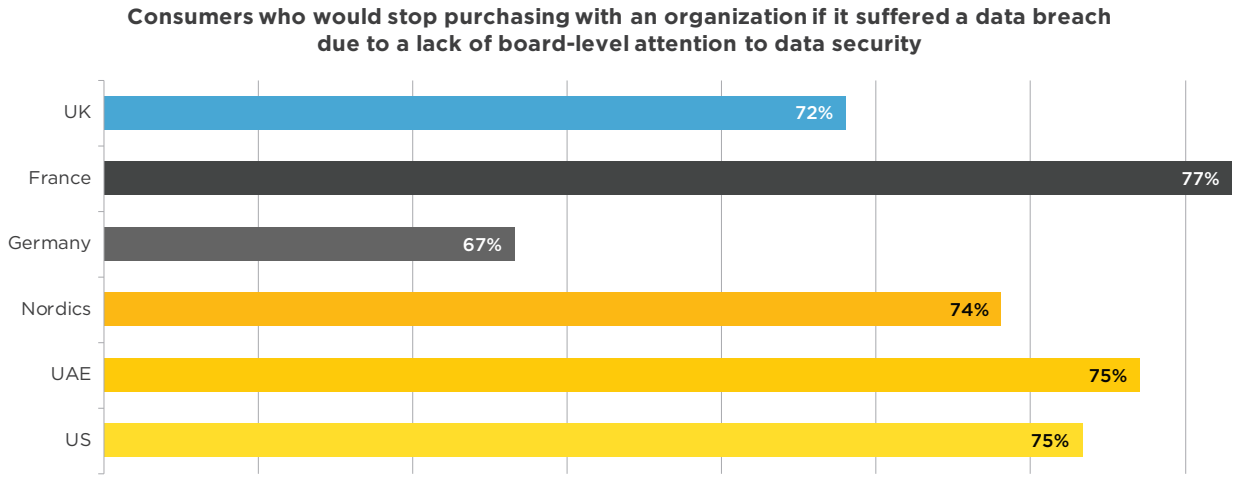
Most consumers expect data security to be at the top of the agenda for organizations and their leadership teams. What actions would consumers take if they were victim of a breach?

FIGURE 7: Analysis of what would be likely to stop consumers purchasing from an organization if they found out it was partially at fault for the theft of their data, asked to all respondents (6500)



Regional insight

FIGURE 7A: Regional analysis of consumer respondents that would stop purchasing from an organizations if they found out it was partially at fault for the theft of their data due to a lack of board-level attention (3161 respondents)



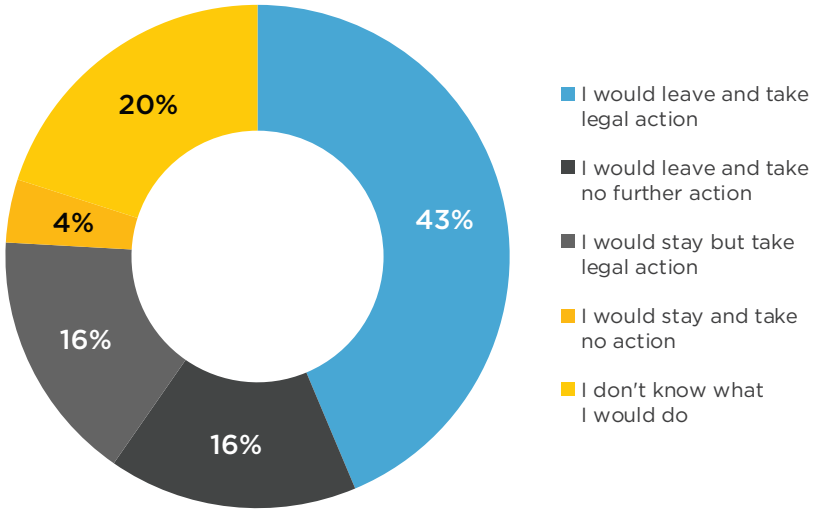
Consumer actions upon experiencing a breach

Six in ten (60%) consumer respondents would take legal action against an organization if their details were stolen and used for criminal purposes as a result of a data breach.

A similar number (59%) would choose to leave the organization involved. Only 4% of consumers surveyed would stay and take no action.

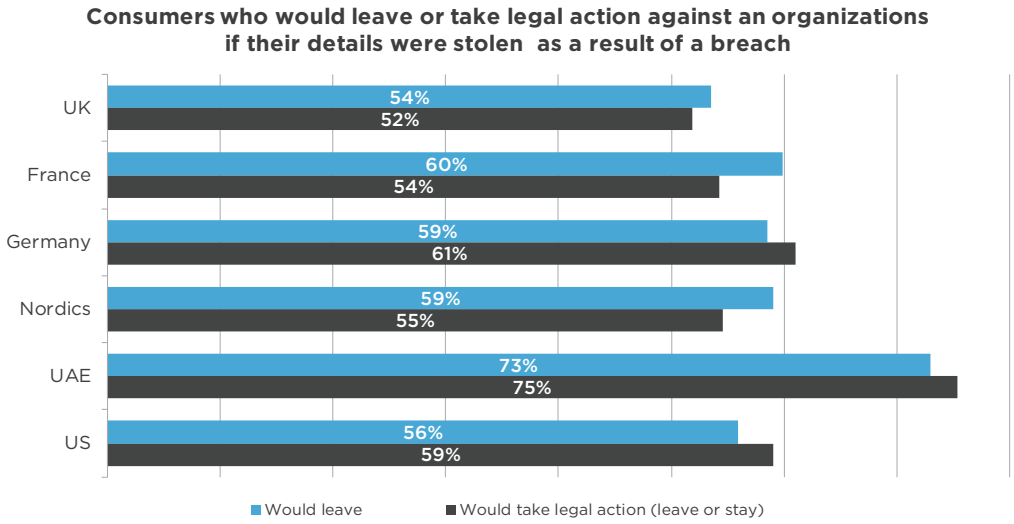
The majority of consumers are willing to take action against breached organizations. How is their willingness to share their personal data being affected by recent cases of data breach?

FIGURE 8: "If yours or your family's details were to be used for criminal purposes as a result of a data breach, how would this impact your decision to remain a customer with the organization involved?", asked to all respondents (6500)



Regional insight

FIGURE 8A: Regional analysis of consumer respondents who would leave or take legal action against an organization which had been breached if their details were stolen and used for criminal purposes, all respondents (6500)



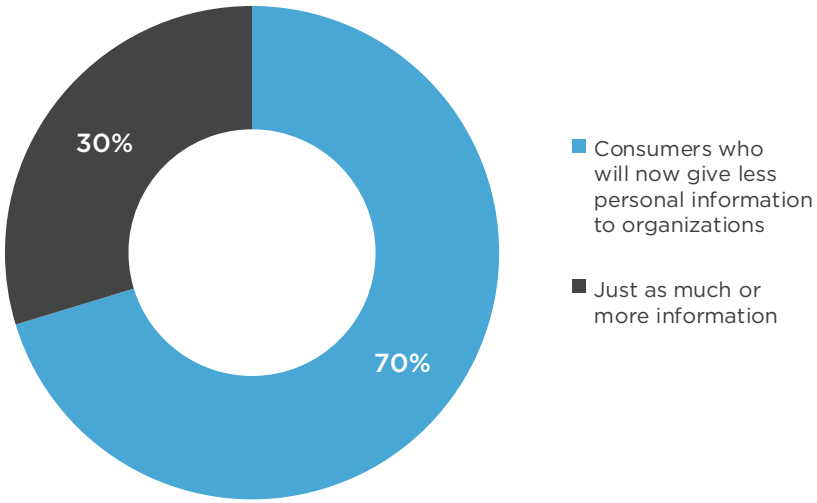
Consumer willingness to share personal data

Seven in ten (70%) consumer respondents would now give less personal information to organizations in light of recent data breaches.

Only three in ten (30%) say they would give the same amount or more.

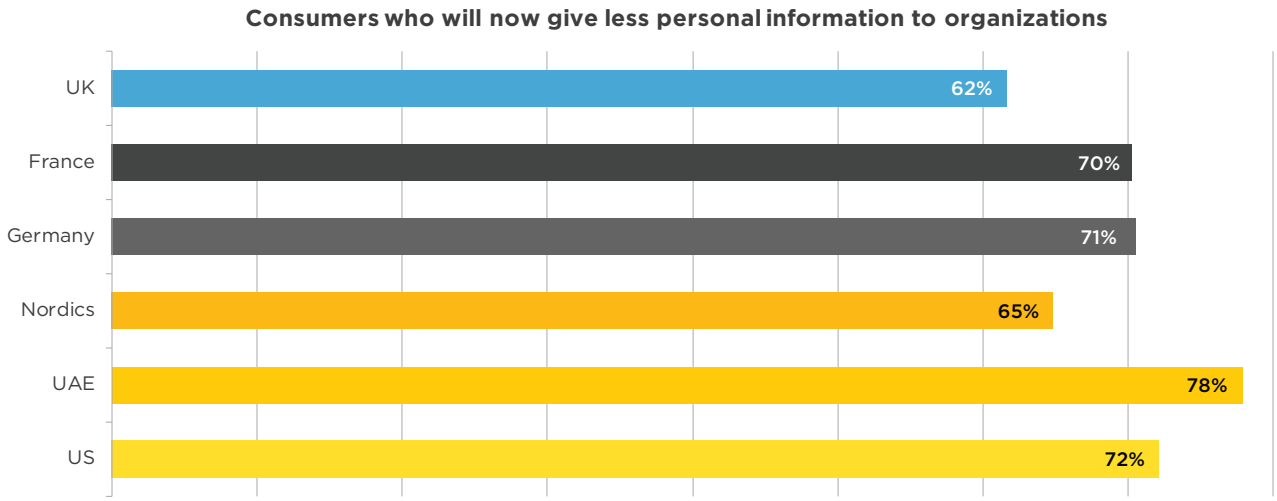
High profile cases of data breaches are causing many consumers to reduce the amount of data they will share with organizations, potentially limiting the ability of these organizations to offer more personalised and tailored products and services.

FIGURE 9: Analysis of consumer willingness to provide personal information to organizations in light of recent breaches that they are aware of, asked to all respondents (6500)



Regional insight

FIGURE 9A: Regional analysis of consumers who will now give less personal information to organizations in light of recent breaches that they are aware of, all respondents (6500)



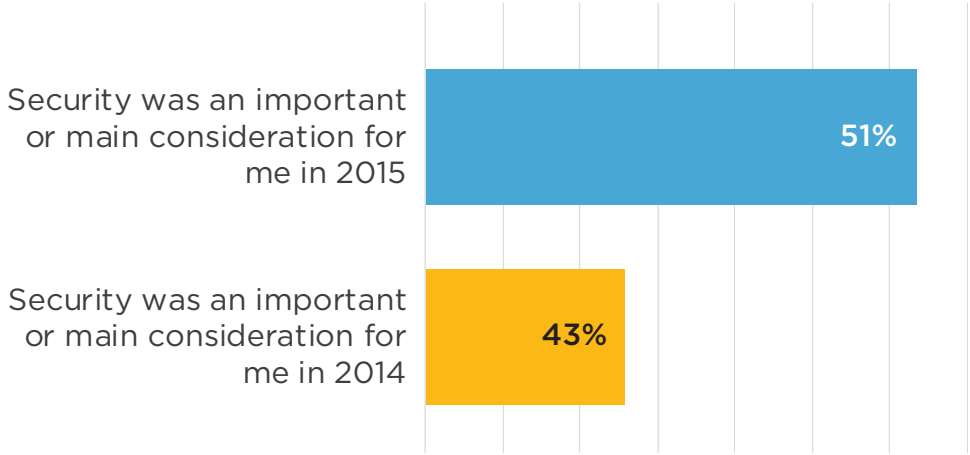
Security as a consideration when purchasing

Just over half (51%) of consumer respondents consider security to be a main or important consideration when purchasing, when thinking about the breaches that occurred in the last 12 months.

This has grown from the previous year, where 43% held security as such a key consideration.

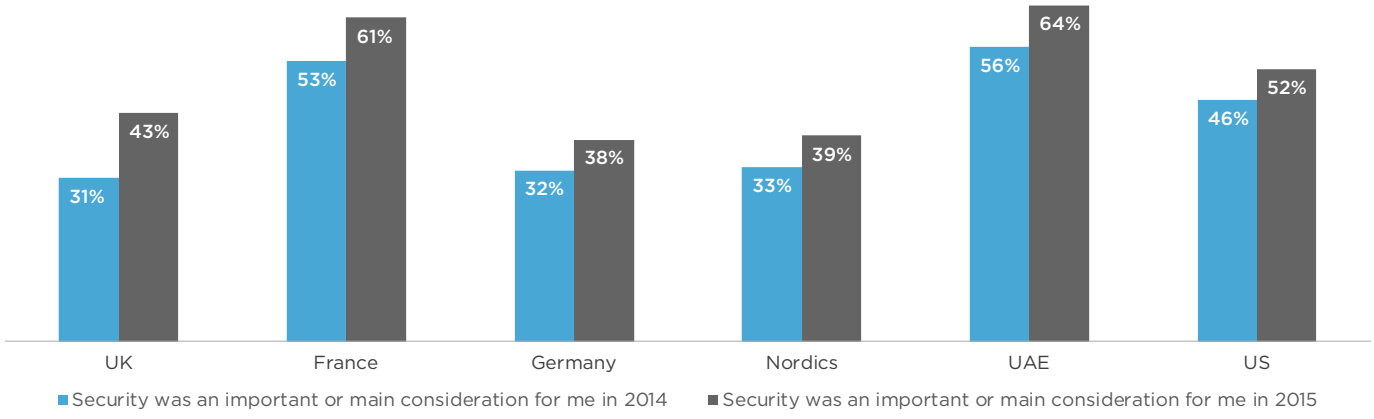
More and more consumers now regard security as a key element of their purchasing decision. This can be a key differentiator for organizations that can demonstrate their security capabilities, but would consumers be willing to pay more to obtain it?

FIGURE 10: With the large amount of high-profile data breaches in 2015, compared to your feelings the year before to what extent was/is data security now something that you would consider when purchasing products/services Analysis of consumers who consider security to be a main or important consideration when purchasing products or services, asked to all respondents (6500)



Regional insight

FIGURE 10A: Regional analysis of consumers who consider security to be a main or important consideration when purchasing products or services, all respondents (6500)



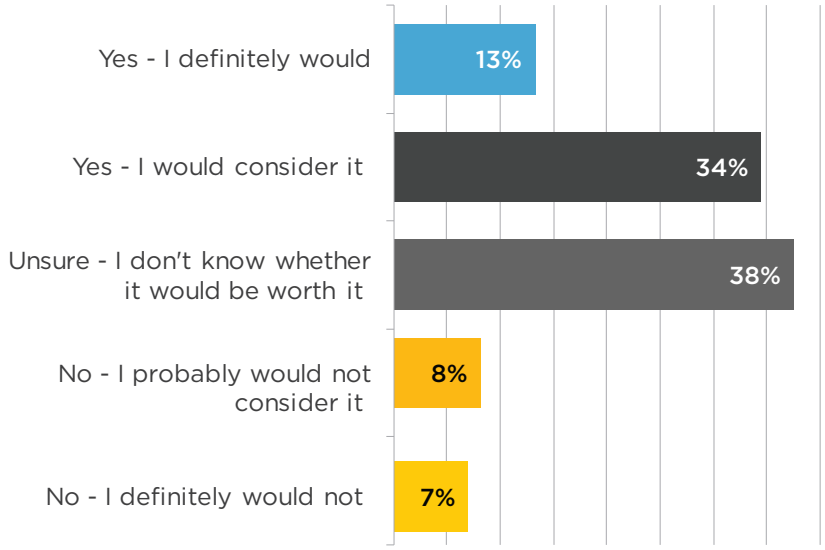
Consumers' openness to paying more for better security

Almost half (48%) of consumer respondents would be willing to pay more in order to work with a provider that has better data security.

Around two fifths (38%) report themselves as unsure as to whether it would be worth it but only the minority (15%) would rule out such action.

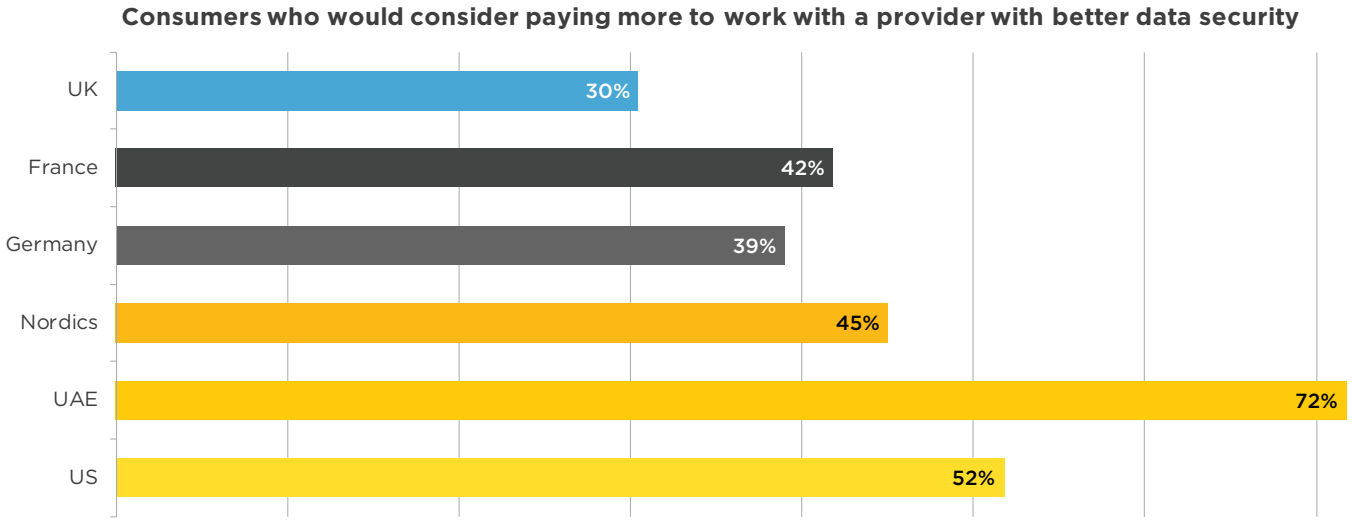
With security forming part of the purchasing decision for more and more consumers (figure 9), as a result many are open to the idea of paying to obtain it.

FIGURE 11: "To what extent would you be prepared to pay more to work with a provider that offered the same products/services but that has better data security?", asked to all respondents (6500)



Regional insight

FIGURE 11A: Regional analysis of consumer respondents who would pay more to work with a provider that has better data security, all respondents (6500)



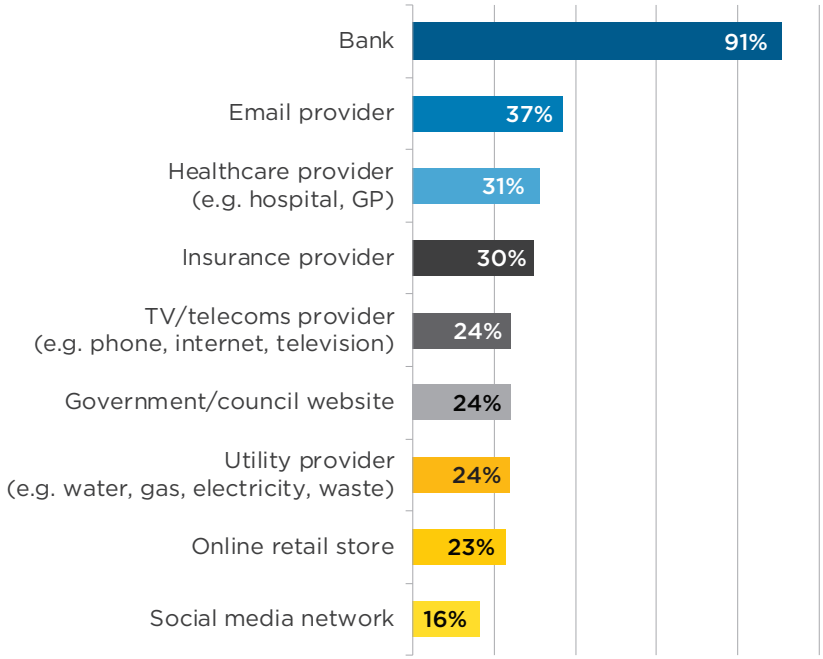
Provider types of highest concern

The vast majority (91%) of consumer respondents would put banks in their top three organization types of most concern if breached.

Three in ten or more would put email provider (37%), healthcare provider (31%) or insurance provider (30%) in their top three.

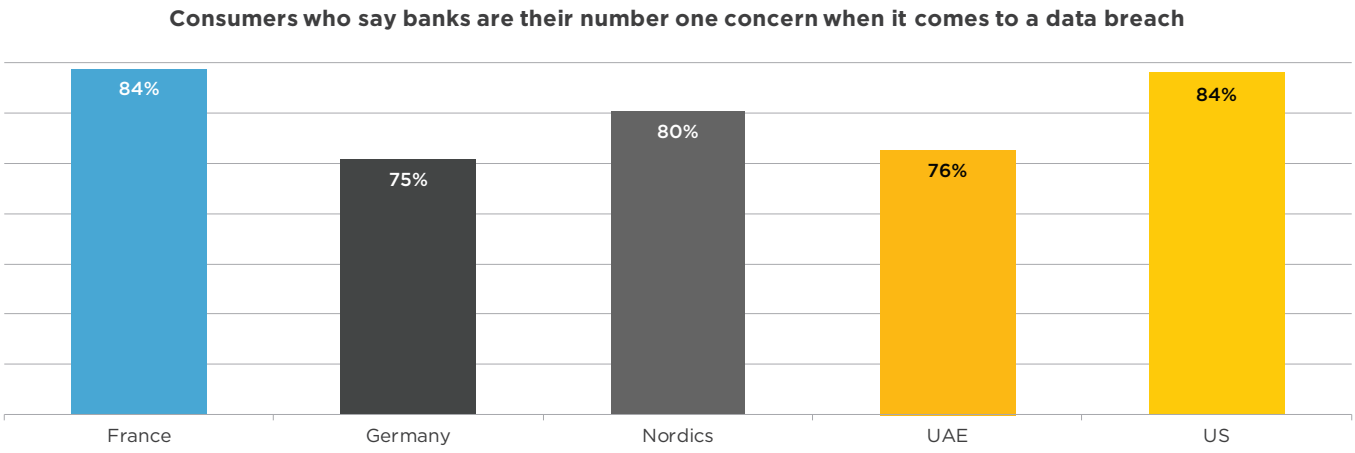
Organizations that hold particularly sensitive financial or personal data are understandably seen as of most concern to respondents.

FIGURE 12: "Which of the following would be of most concern to you if they were the victim of a data breach, potentially exposing your details to cyber-criminals?", asked to all respondents (5500 – not including UK)



Regional insight

FIGURE 12A: Regional analysis of consumer respondents who say that banks are the number one concern when it comes to a data breach, all respondents (5500 – not including UK)



Note: this question was not asked to UK respondents

Summary

- Two thirds (66%) of consumer respondents expect to be informed immediately if a data breach occurs.
- Close to half (46%) report that they have a full awareness and understanding of the potential impact that a data breach can have.
- A quarter (25%) believe that their data would be less secure with an organization that has been breached compared to an alternative supplier.
- Close to four in ten (36%) say that their perception of breached organizations has diminished.
- A third (33%) now feel more negatively about organizations in general as a result of high profile data breaches.
- Around three quarters (73%) report that they would be likely to stop purchasing with an organization if they found out that the theft of their data was due to a lack of board-level attention to security.
- Six in ten (60%) would take legal action against an organization if their details were stolen and used for criminal purposes as a result of a data breach.
- Seven in ten (70%) consumer respondents would now give less personal information to organizations in light of recent data breaches.
- Just over half (51%) now consider security to be a main or important consideration when purchasing.
- Almost half (48%) would be willing to pay more in order to work with a provider that has better data security.
- The vast majority (91%) would put banks in their top three organization types of most concern if breached.

Key Regional Differences

- More consumer respondents in the Nordics (70%) and UAE (70%) expect to be informed immediately of a data breach.
- The perception and loyalty of consumer respondents in the UAE (45%,38%) and the U.S. (41%, 36%) has diminished the most towards the organizations affected by data breaches.
- Consumer respondents in the U.S. and UAE are also more likely to feel more negatively about organizations in general as a result (43% and 36% respectively).
- UAE consumer respondents in particular are much more likely to take action against organizations if their personal details were stolen and used for criminal purposes — around three quarters would take legal action (75%) or leave the organization involved (73%).
- U.K. consumer respondents remain slightly more open to sharing their personal information with organizations – 62% will now give less – whereas 78% of UAE respondents will give less.
- Over six in ten consumers in France (61%) and UAE (64%) now consider security as a main or important consideration when purchasing.
- U.K. consumers (30%) are least likely to consider paying more to work with organizations that offered better data security, whereas seven in ten (72%) UAE consumers would be open to doing so.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com