In this the fifth issue, we share the findings of some brand new research into the consumer response once a data breach has been discovered. The research tells us very clearly how consumers feel a company should respond post data breach and also is a very clear indicator of how consumer behaviour adapts after a company has a data breach.

## The Objectives

This round of research was focused on understanding consumer response after awareness of a data breach. The questions we asked were the following:

1. If a company had had a serious loss of its customer data to what extent would that affect your likelihood of doing business with them?
2. If a company had a serious data loss, that you weren't currently a customer of, how might it impact your future buying decisions?
3. How should the company communicate that it has had a data loss to the public and affected customers?

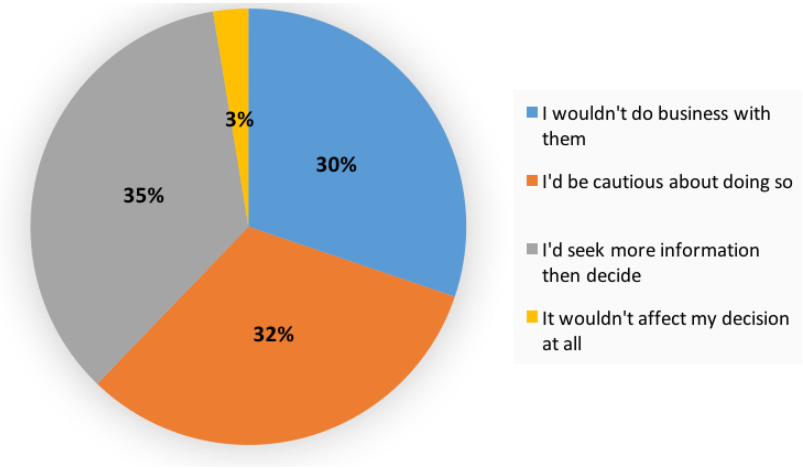
## Methodology and sample

In order to get a robust, representative spread of respondents, we used a specialist consumer engagement platform, OnePulse, which enables quick market research by sending little bite-size surveys known as 'pulses' to its panel via a mobile app. We sent the 'pulses' to a cross section of individuals from the entire UK based panel to secure a statistically robust and representative sample of the wider population. We stopped the research when we had secured 1,000 respondents providing a margin of error of c. +/- 2.7%. Amazingly, all responses were received within 1 hour 21 minutes.

# Research findings

**Question 1: If a company had had a serious loss of its customer data to what extent would that affect your likelihood of doing business with them?**

Our research uncovered that if a company lost customer's data only 3% stated that it would not affect their future decisions to do business with the company. That leaves a dramatic 97% of people THAT WOULD alter their behavior as a result of a data breach. A significant 30% of respondents stated that they wouldn't do business with the company again, which if replicated would have a significant impact on company financial performance.




The largest proportion of respondents, at 35%, stated they would seek more information before deciding whether to continue doing business with a company. This strongly suggests that customers would alter their opinions based on the 'circumstances the breach' indicating that the tone and positioning of initial announcements within the media are critical and, as always, that first impressions count. This provides a breached entity with the clear opportunity to influence customers towards a more lenient response in their future decision making, if the breach was portrayed unpreventable and that the company was the victim of crime rather than remaining 'open' to criminal activity.

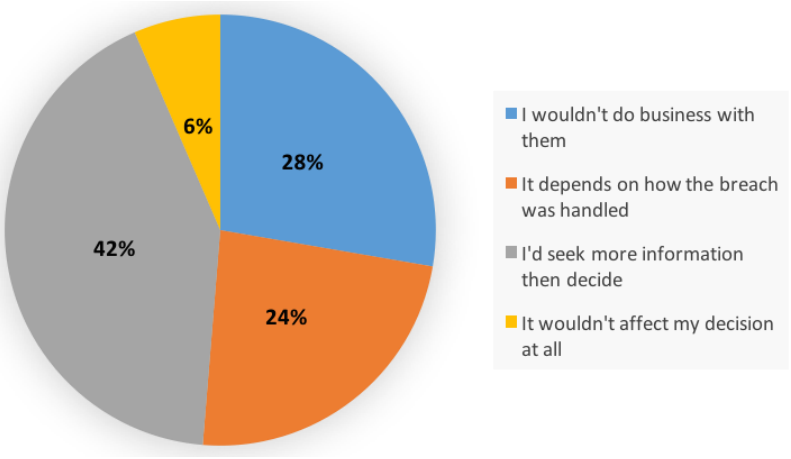
In addition, almost one in three respondents (32%) stated that they would be cautious in doing business with a company that had had a serious data breach. This is a group in which we can't definitively state whether or not they would continue to transact at the same level as pre-breach. What can be clearly concluded is that a significant amount of thought would now go into a future decision to transact. The result may involve consumers going to alternative suppliers for the same product. Alternatively the consumer may continue to transact in a more cautious manner, which may involve using a new specific payment card or new email address for contact. Whilst this may appear to impact little on top and bottom line performance, such behaviour may indicate a level of trust had been lost, indicating a potential loss in the long term value on the customer relationship.

What is also interesting is the significant difference between the answers to the similar question reported in our October 2015 White Paper addressing consumer response to Payment Card Fraud. In that study 68% of those questioned indicated that they would significantly alter their future purchasing behaviour, against the 97% of respondents in this study responding to the question on personal data indicating a much greater concern on personal data fraud rather than payment card data.

Our next pulse of research explores these differences further. Watch this space.

## Question 2: If a company had a serious loss of data, that you weren't currently a customer of, how might it impact your future buying decisions?

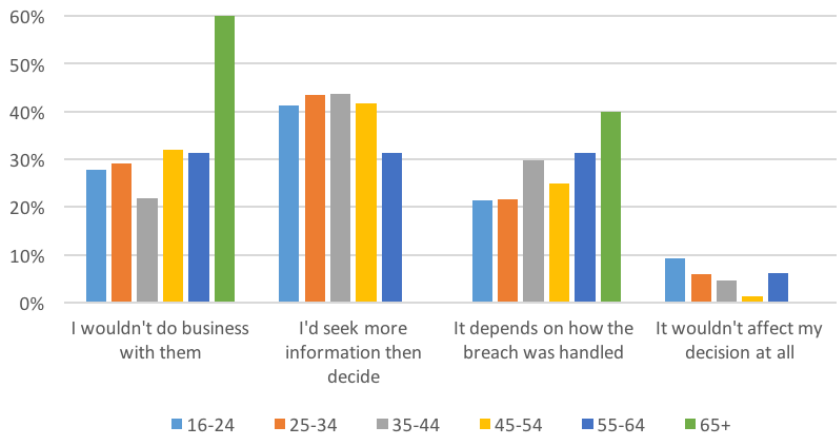
Here we look to see if our respondents would behave any differently to a company's data breach if they were NOT currently a customer of the targeted business.




It can be seen that almost 1 in 4 respondents (24%) indicated that they would base their future buying behavior specifically on how the breach was handled. This response provides a significant opportunity to give potential customers confidence and provide a basis for future growth stressing the importance of a data breach response planning to offset the potential damage of breach.

We can also see that 42% of respondents NOT already customers would seek more information and conduct research before future buying decisions were made. This is note-worthy because it indicates that an additional 7% of respondents would conduct research into a company that they were not a customer of rather than one they already traded with potentially emphasizing that customers trust the company they do with business with and that this trust should not be abused.

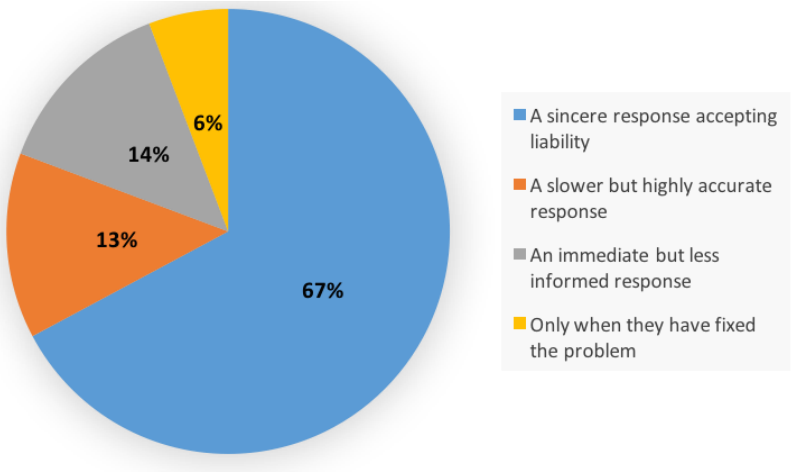
It is also significant to point out that double the amount of consumers (6%) that don't already trade with a business wouldn't let a data breach affect their decision at all. This could be down to the point that they were not inclined to do business before and certainly wouldn't now, alternatively they haven't personally had their data at risk so wouldn't put this against a company and alter their future buying decisions. Studying the data in more depth, 60% of respondents in the '65+' age group wouldn't do business with a company that had lost customers data. This emphasizes how much the older generations fear their data being lost.




Another noteworthy extraction is within 'I'd seek more information then decide'. Just over 40% of 16-54 year olds would all seek more information before deciding whether to do business with a company that had breached their customers data whereas 10% less of '55-64' year olds would. Which shows that the older generations are less likely to research the breach before altering their behaviour.

## Question 3: How should the company communicate that it has had a data loss to the public and affected customers?

This question focused on how customers wanted companies to report its data loss to general public. We allowed comments on this question to get a more in depth insight into how consumers feel. Interestingly a 45-54 year old male from the midlands that wanted to see a sincere response accepting liability stated that *"Talk Talk's recent response was too quick and ill informed".* Whilst the General Data Protection Regulation (GDPR coming into effect in May 2018) will require entities to report a data breach to those impacted within 72 hours of discover, this response suggests that statements can be too rapid; it notes that though customers prefer not to be left in the dark, depth of information is key. This ties into another comment we received from a similar but slightly younger respondent stating: *"I think an immediate response is important especially to the users, but it can't be light on detail. There needs to be an understanding of what's been breached and what is lost. Uncertainty can cause panic!"* These comments are extremely useful in gaining insights into consumer thoughts. Another comment from a 25-34 year old male from London that wanted an immediate but less informed response was quoted saying: *"It would be good to know if you are personally affected".* This again emphasizes that point that depth of communication is key to informing customers when a breach takes place.




The results seen from this question clearly show 2 in 3 people would want a sincere response accepting liability. Consumers do not want to see the blame being passed around when a breach has occurred. They want to know that the business takes responsibility for the loss of their data and does all it can to protect it. A similar percentage of people are seen to request a slower, accurate response compared to an immediate less informative response. This highlights the possibility that time of response isn't the most important factor as far as the customer is concerned, and that accuracy and depth of information is key.

Along with the comments we received, the conclusion can be made that as soon as companies are aware of how many and hopefully whose data has been lost, informing these consumers is the main priority. This is supported by a very small percentage (6%) of people only want to be notified once the issue had been resolved. This stresses the point that majority consumers want to be informed about the issue earlier than the resolution of the problem.

# Conclusions and implications

This new update of our research initially reveals that respondents are more likely to alter their purchasing behaviour if personal data is lost over payment card data. This could be due to the associated risks with personal data fraud though the reasons behind this will be uncovered in our next round of research.

Our research also shows that the large majority (97%) of customers of a company experiencing a data breach would potentially alter their purchasing behaviour as a result of that data breach. This emphasizes the importance in companies doing all they can to protect customers data, as doing so will have a beneficial outcome.

Our research confirms that post breach behaviour is very important in retaining customers on the fence. It shows that customers clearly want to see businesses accepting liability with a sincere response post-breach. Respondents are also very keen to be informed as soon as the breached company is aware of how many and whose data has been breached in order to reduce panic. Though rapid customer communication is desired, it can be noted that media announcements need to be well planned, informative and fully considerate of consumer segments and their consumers likely responses to those media announcements.

Don't risk it.

Contact us for more information on how Compliance3 can support your own breach response planning and response preparation by providing access to core response data and initiating immediate communication to your existing customers as part of your incident response and business continuity team.

# Further consumer research

For the results of earlier rounds of consumer research, please visit our website

http://www.compliance3.com