

# The People VS e-Commerce – Consumer Attitudes to Data Security

## Contents

2	<b>Introduction</b>
2	<b>About the Survey</b>
2	<b>Executive Summary</b>
3	<b>Key Findings</b>
3	Q: What types of information are you most bothered about protecting?
3	Q: Who would you like to see being more proactive about protecting your data?
3	Q: Do you expect a bank, building society or other institution responsible for loss of your information to notify you automatically?
3	Q: How would you react if a retailer, bank or other institution lost your personal information?
3	Q: There is a big rise in the sale of personal data to external sources often for criminal or illegal activity. Do you worry about the ability of data centres to protect your data?
4	Q: Do you feel that online e-commerce sites, banks and retail outlets do enough to protect your personal data?
4	Q: Have you ever been a victim of data theft?
4	Q: Which one of these statements best describes your attitude about giving out personal information online?
5	<b>Conclusion</b>



## Introduction

The last few years have witnessed significant changes on the hacking landscape, and no bigger change can be found than in the motives of hackers. Traditionally, hackers were little more than script kiddies that indulged in cyber-vandalism – corrupting or deleting files etc – to earn kudos from the hacking community.

Today, the criminal underground occupies the scene, harbouring far more sinister designs. Cyber-villains have been attracted by the huge amounts of money that can be made from targeting corporate databases using sophisticated hacking techniques to steal personal data, which can then be used to commit identity fraud and plunder money from victims' accounts.

Security professionals are engaged in a perennial game of cat and mouse, thwarting daily individual, targeted attacks that are crafted to steal the lucrative personal details of consumers from company databases. Unfortunately, however, not all security products and services are sophisticated enough to detect and prevent all of the attacks that specifically target company databases.

High profile security breaches have brought the issue of protecting customers' personal details to the public's attention like never before. TJX Companies, which operates discount retail chain TK Maxx in the UK, announced in January 2007 that account information from 45.7m credit and debit cards, and identity data belonging to 455,000 individuals, had been stolen in hacking attacks between 2005 and 2007. The fallout was significant. The privacy and information management research company, Ponemon Institute has found in its annual survey on the cost of data breaches<sup>1</sup> that a data breach costs companies an average of \$182 per record, a 31 per cent increase over the previous year. The eventual cost of TJX's breach is likely to run into the billions of dollars; dwarfing the \$25m costs the company itself has confirmed it knows it has incurred so far. Of course, much of the cost will be carried by other companies, such as the credit card suppliers forced to issue so many replacement cards.

Consumers are now waking up to the fact that their personal details, held on databases by hundreds of organisations, are not necessarily secure and are vulnerable to attack from determined criminals.

But to what extent have such high-profile events really entered the consciousness of the general public? Secerno sponsored independent research by Ipsos MORI which reveals the public's attitude towards e-commerce transactions, data protection, and database security. The findings provide invaluable insight to consumer expectation and demand – and urge banks and other e-commerce organisations to re-appraise their security policies.

## About the Survey

A national representative sample of 1,243 UK adults aged 15+ were interviewed between 23rd March and 29th March 2007. All interviewing for Capibus is carried out in-home by Ipsos MORI interviewers using CAPI (Computer Assisted Personal Interviewing).

## Executive Summary

Data theft is evidently a far-reaching transgression – just over one in 12 consumers have been victims of this crime.

When it comes to protecting personal details, money talks – people are more concerned about protecting their bank and credit card details (83 per cent) than any other type of information, including their medical records (46 per cent) and even data about their children (35 per cent).

Consumers are very clear on which organisations are letting them down. Forty-five per cent of consumers believe that e-commerce sites, banks and retail outlets are not doing enough to protect their data. Consumers are also unequivocal about which bodies should be seizing the initiative and taking a more proactive approach to protecting their personal details – the government and banks.

Banks and other financial institutions were handed a strong warning: the vast majority of consumers (82 per cent) expect to be notified immediately if there has been a security breach and their personal details have been compromised. Trust in banks and building societies to protect personal details is incredibly low – just four per cent have faith in such financial institutions to keep their details safe.

However, the poll also highlighted why financial institutions are reluctant to follow the US's lead and publicly disclose a loss of personal data. Upon hearing of a data breach, most consumers (53 per cent) would vote with their feet and stop using the institution's services immediately. And many consumers would take the matter higher to ensure further action is taken on their behalf: one-fifth would report the matter to the police as criminal matter, while 17 per cent would notify the relevant consumer watchdog of the incident.

Data centres also elicit a cynical response from consumers. Nearly two-thirds (63 per cent) believe that data centres are ill-equipped to protect their personal details.

Concerns over online security are seeping through to consumers' actions – more than one-third said there are some personal details that they would simply never submit online, while 13 per cent of consumers never shop online.

## Key Findings

### **Q** What types of information are you most bothered about protecting?

The biggest concern when it comes to protecting information is the need to safeguard personal banking or credit card details. A massive 83 per cent of respondents claimed they are concerned about keeping this information safe. Concern increases among high-earners (more than £25,000), with the figure rising to 96 per cent. Respondents in the higher age brackets, 45-54 (88 per cent), 55-64 (89 per cent) and 65+ (86 per cent) express notably more concern about protecting bank and credit card details than those in the lowest, 15-24 age group (75 per cent).

Protecting NHS or other medical records is important, cited by 46 per cent of respondents. Again, respondents in the higher age brackets, 45-54 (52 per cent), 55-64 (56 per cent) and 65+ (49 per cent) express more concern about such details than the lowest, 15-24 age group (39 per cent).

The third greatest concern is about lifestyle data, cited by 40 per cent of respondents.

A little more than one-third of respondents (35 per cent) expressed concern about their child's personal details being kept secure; while an almost identical amount (34 per cent) are concerned about protecting information held by marketing companies or other third parties.

Respondents that are married, have children and are working generally expressed more concern about protecting each of these categories.

### **Q** Who would you like to see being more proactive about protecting your data?

More than half of all respondents believe that the Government (58 per cent) and banks and building societies (58 per cent) should be doing more to ensure their data is secure.

A little under half (47 per cent) believe that retailers should be taking more responsibility when it comes to data protection.

A little under a quarter (22 per cent) of respondents believe that the council could be more proactive when it comes to protecting consumers' data.

Fifteen per cent would like independent regulatory bodies, such as consumer watchdogs, to take a more active role; while 12 per cent would like help from overseas with a more proactive approach from the EEC.

### **Q** Do you expect a bank, building society or other institution responsible for loss of your information to notify you automatically?

The vast majority (82 per cent) of respondents were unequivocal and said they should be notified immediately if a bank, building society or other institution had lost their information. Higher earners were even clearer in their response, with 93 per cent demanding an immediate disclosure. The older age brackets, 45-54 (87 per cent), 55-64 (89 per cent) and 65+ (85 per cent), were more insistent on transparency when personal details have gone awry than the lowest, 15-24 age group (78 per cent).

A mere seven per cent expect to hear about a loss of their personal information 'eventually'.

Just four per cent said they trust banks and building societies to look after their personal details.

### **Q** How would you react if a retailer, bank or other institution lost your personal information?

More than half of respondents (53 per cent) would not give the institution another chance and would stop using its services immediately. A little less than half (48 per cent) would take preventative measures and would cancel all their credit cards.

One-fifth (20 per cent) would take the matter higher and would notify the police.

Seventeen per cent would inform the appropriate consumer watchdog.

Only two per cent claimed that they would take no action if their details were lost.

### **Q** There is a big rise in the sale of personal data to external sources often for criminal or illegal activity. Do you worry about the ability of data centres to protect your data?

Nearly two-thirds (63 per cent) of respondents worry that data centres are ill-equipped to protect their data.

The 45-54 age group expressed the most concern (74 per cent), while the youngest bracket, 15-24, was considerably less worried about data centres (45 per cent).

Married respondents (69 per cent) showed more anxiety about data centres than unmarried respondents (55 per cent).

Three-quarters of higher income earners (£25,000+) are wary about data centres compared to three-fifths of lower income earners.

**Q Do you feel that online e-commerce sites, banks and retail outlets do enough to protect your personal data?**

A little under half of respondents (45 per cent) believe that e-commerce sites, banks and retail outlets are not doing enough to protect their data. Just under one-third (29 per cent) claim that they are doing enough, while 26 per cent are undecided.

Again, the oldest and youngest age groups' responses varied markedly. The 15-24 group have more faith in e-commerce sites, banks and retail outlets, with 41 per cent believing that such organisations do enough to protect users' personal data, compared to just 12 per cent of those in the 65+ bracket.

Respondents on a high income, £25,000+, were more content that these organisations are doing enough to protect their personal data (39 per cent) than those on low incomes, up to £11,499, (23 per cent).

**Q Have you ever been a victim of data theft?**

Nearly one in 12 (eight per cent) respondents have been a victim of data theft.

The age group most likely to fall victim to data theft is 45-54 (15 per cent).

Men (10 per cent) are more likely to be victims of data theft than women (seven per cent)

Respondent that earn more than £25,000 are more likely to be victims (14 per cent) than those who earn lower incomes (five per cent).

**Q Which one of these statements best describes your attitude about giving out personal information online?**

A little more than one-third (36 per cent) of respondents claim that there is some information that they would never put online. Again, there was some disparity among age groups, with the figure rising to 49 per cent among 45-54-year-olds and dropping to 33 per cent among 15-24-year-olds.

A little more than one-fifth (21 per cent) never use online banking, with the figure rising to 17 per cent among 15-24-year-olds.

Seventeen per cent claim that there is some information that they regularly give out online.

Thirteen per cent never shop online.



## Conclusion

The findings of the survey make stark reading for e-commerce organisations, banks and other financial institutions. High profile data security breaches have evidently rocked consumers' faith in the ability of large organisations' ability to protect their personal data. Consumers are demanding that they be informed immediately whenever a breach occurs. Worse, the public are clearly unafraid to take the most damaging action – withdrawing their custom immediately if a security breach is uncovered. There is a clear danger that online and offline sales could diminish beneath this tide of public cynicism.

Companies holding personal data are aware that the ramifications of a security breach are severe. Unsurprisingly, they are reluctant to disclose to the public when they have been victim of an internal or external attack for fear of the effect it will have on brand reputation, the cost of the clear-up, and the inevitable negative impact on share price.<sup>2</sup>

Clearly, there is a need and a demand from consumers that the Government and the EU should follow the US's lead and impose a legal framework that forces companies to disclose security breaches. Currently, a situation that mirrors the TJX breach may already have happened in Europe, but companies operating in this region would not be legally obliged to notify their customers – which only serves further to erode public confidence.

However, organisations should not simply passively await the appropriate legislation. Wise companies should seize the opportunity not only to reverse the swell of negative public opinion, but also steal a march on their competitors by placing database security at the heart of their operations.

Ensuring personal details are secure should be a company's first priority – to place database security at the heart of a company's security strategy is to place customers at the heart of the security strategy. In so doing, companies can set themselves apart from their competitors: they can not only ensure that *their* systems are never compromised again but also, assure their *customers* that *their* personal details are held as securely as possible so that they will not be victims of data theft.

Today, there are database security solutions on the market that allow companies to achieve this realistic goal. Only in so doing will companies be able to prove to the public that guaranteeing the protection of their personal details is of paramount importance, which will help rebuild consumer confidence and, ultimately, drive business growth.

Cross-Bench Peer and Secretary to the All Party Internet Group, Lord Erroll<sup>3</sup>, comments: "People should demand that organisations prove that they are taking reasonable steps to protect their data, such as adhering to the international standard for information security ISO 27001 (BS7799), under which all data should be encrypted and protected by rigorous identity management and access controls.

"Organisations should ensure that they track the activity of every person who has access to personal data to make sure that they are not using it inappropriately.

"Also, data should not be held in one large database; if all of the data is concentrated in one place, the risks are far greater. It is preferable that organisations use a federated data model with lots of data silos so that if one set of information is stolen, it is only part of a person's identity that has been compromised.

"Now is the time for all organisations to show that they are taking the protection of our personal data very seriously before it is too late."

<sup>2</sup> Templeton College, Oxford University study of affect of data breaches on market capitalisation found a serious security incident could affect share price by 5 – 10%

<sup>3</sup> The Earl of Erroll is a Cross-Bench Peer and is Secretary to the All Party Internet Group ([www.openrightsgroup.org/orgwiki/index.php/All\\_Party\\_Internet\\_Group](http://www.openrightsgroup.org/orgwiki/index.php/All_Party_Internet_Group)) and is also on the ISSA UK Executive Advisory Board (<http://issa-uk.org>). He sits on the Local Authority Smartcard Standards e-Organisation (LASSSEO) ([www.lasseo.org.uk](http://www.lasseo.org.uk)), is a member of the European internet security lobbyist EURIM ([www.eurim.org.uk](http://www.eurim.org.uk)), is president of the E-business Regulatory Alliance ([www.e-ra.org.uk](http://www.e-ra.org.uk)) and has a background in computer security and identity management.

## About Secerno

Award-winning Secerno provides the world's most advanced, comprehensive and intelligent database security solution.

Deploying a microperimeter approach, Secerno SQL sits right next to an organisation's data asset to protect data at the highest level. Its unique machine-learning technology understands the true intent of database interactions and protects an organisation's data from both known and unknown threats to data, whether they originate from external or internal sources.

Located in Oxford, UK, Secerno enables the continuous improvement of data security by allowing companies to understand, control and protect their data assets. It empowers organisations to derive the most value from their information and to enable data security without the costs associated with traditional solutions.

Secerno offers protection to customers across an array of industries including financial services, healthcare and pharmaceuticals, retail and government agencies and departments. Secerno is funded by UK investors, including Eden Ventures, Quester and Oxford Venture Management, who have a successful track record for backing winning innovators and entrepreneurs.

For more information about Secerno visit [www.secerno.com](http://www.secerno.com), email [enquiries@secerno.com](mailto:enquiries@secerno.com) or call +44 (0)845 450 9460.



Secerno Limited, Seacourt Tower, West Way, Oxford OX2 0JJ T: +44 (0) 845 450 9460 E: [enquiries@secerno.com](mailto:enquiries@secerno.com)