

Deloitte.

Take the longer term view
Consumer Business
Security Survey 2009



Contents

1	Foreword
2	About the survey
3	Key findings
4	The general state of security
6	Threats, vulnerabilities and impacts
8	Third parties
10	Training and awareness
12	Data quality
13	Conclusion

Foreword

Despite the economic climate negatively impacting Consumer Business (CB) organisations, security issues remain high on the agenda. In what may be a rare piece of good news for the industry this year, we have seen real improvement in several areas of security over the past twelve months – a recognition perhaps that media coverage on data loss incidents still has the attention of senior management.

The second edition of Deloitte's annual Consumer Business Security Survey allows companies in the industry to understand current security issues and provide a benchmark to their peers.

There are a number of reasons why security is critical to CB organisations:

- Consumers trust retailers with a considerable volume of personal and financial data. They expect CB organisations to protect their data to the same standard as a bank. When companies breach that trust, the effects can be devastating to the brand. Retailers cannot afford to lose any custom in the current market.
- Many organisations are heavily focussed on reducing costs and improving liquidity. Poor quality data generates considerable inefficiencies in processing and impacts on the accuracy of management information. With data volumes rising by 50% per year*, the data is there in abundance – but management don't trust it and struggle to derive value from it.

* Why database archiving should be part of your DBMS strategy, quotation from a commissioned study conducted by Forrester Consulting on behalf of Clearpace, January 2008.

- Third parties form a core part of any supply chain, and now have increasing responsibility for handling and processing sensitive data. Understanding the risks associated with third parties and managing these effectively, whether that be in maintaining continuity of supply or protecting confidential data, is critical. Organisations have started to consider these risks more formally, but few currently assess the effectiveness of the controls in place around these third parties.

Deloitte's 2009 Consumer Business Security Survey identified the security issues and threats that are of the greatest concern to CB companies. The survey highlights the measures businesses are taking to avoid security breaches and ensure compliance.

Thank you for your time and participation. We hope you find the report useful.



Mike Maddison
Head of UK Security & Privacy

About the survey



Specific interview topics included:

- Governance, structure and investment
- Strategy and initiatives
- Threats, vulnerabilities and impacts
- Incident detection and management
- Technologies
- Training and awareness
- Third parties
- Business continuity planning
- Data quality
- Compliance

Deloitte undertook a survey in the UK to help CB companies benchmark their security practices against their peers. Data was collected through discussions between Deloitte's CB security specialists and security management from consumer business companies. This second annual edition of the survey saw a significant increase in responses, with the involvement of some of the UK's largest retailers and consumer goods businesses. This year's survey has again crossed borders to include responses from three Swiss businesses.

Respondents were typically: Chief Information Security Officers (CISO), Information Security Managers, Chief Security Officers (CSO) or IT Directors. Retailers made up 48% of respondents and consumer goods businesses 35%, with the remaining 17% of surveys completed by businesses operating in the business service sector.

Key findings

- Over half of the companies interviewed have experienced project cuts as a result of the economic downturn.
- 91% of consumer businesses have experienced at least one information security breach in the last 12 months, a 27% increase on last year.
- 48% of CB companies anticipate that social engineering will be a major threat to security in 2009.
- 96% of consumer businesses have third parties with access to their customer data.
- 57% do not carry out periodic security assessments once third parties have been engaged.
- 74% of companies do not have a defined information security training and awareness programme.
- 43% of CB companies have a formally defined information security strategy, compared with 20% last year.

Top five threats envisaged in 2009:

- Social engineering
- Theft or leakage of internal data
- Employee misconduct
- Virus/worm outbreaks
- Weak passwords

Top five security initiatives:

- Regulatory compliance
- Data leakage
- Reporting and measurement
- Infrastructure improvement
- Governance

The general state of security

The need for diligent security practice has never been greater than during this time of increased economic uncertainty. The CB Sector has been hit particularly hard, with slowed growth, decreasing profits and an increasing number of high-profile insolvencies. The results of the survey show that while relative investment in security is expected to maintain an upwards trend, the immediate effects of the economic downturn are putting pressure on security and technology budgets.

The impact of the economy on security budgets has the potential to negatively affect security and compliance initiatives over the coming year. 55% of respondents have experienced project cuts as a direct result of the credit crunch and 30% expect budget cuts in 2009. When asked about plans to fulfil PCI DSS* compliance, 79% of respondents processing card payments said that they have started programmes to do this. With 45% of companies planning to meet PCI requirements and estimating spending in excess of £1 million**, any budget and project cuts are likely to cause delays in achieving compliance.

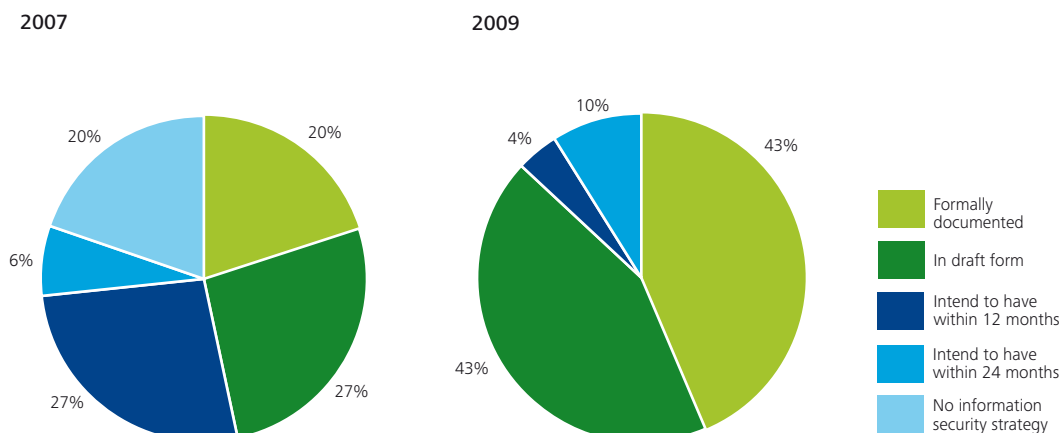
The focus of our 2007 CB security survey*** report was the tactical (rather than strategic) approach that businesses were taking to information security. This year's results indicate that businesses are beginning to trend toward a more strategic approach to security with 43% having a formally documented information security strategy, compared to 20% in 2007 (see figure 1). The remaining respondents had security strategies in draft form (43%) or intended to have one within the next 24 months (10%), a sign of maturity when compared to the 20% of 2007 respondents with no intention

of developing a strategy. Although this is a marked improvement since 2007, consumer businesses still lag considerably behind the Financial Services Industry (FSI) in the formal development of both security strategies (61% of FSI companies have a formally documented strategy) and governance frameworks (45% in CB, compared with 69% in FSI****).

The list of the top five security initiatives saw important changes from 2007. Regulatory compliance, governance and infrastructure improvement feature in both. Reporting and measurement was an addition to the top five list, perhaps indicating an awareness that managers will have to provide better evidence of the security function's value to the business in order to win funding in the current economic climate. The top positioning of regulatory compliance and data leakage highlight the importance consumer businesses place on fulfilling their data security obligations. The inclusion of data leakage as one of this year's top security initiatives is also likely to be a reflection of continued media focus on data loss and subsequent damages caused. Security strategy also remains a high priority, providing an encouraging sign that consumer businesses understand that security programmes must be continually evolved to provide current and effective risk mitigation to prevent security breaches or financial loss.

* Payment Card Industry Data Security Standard (PCI DSS)
 ** Swiss companies responses were given in CHF. The exchange rate used was 1 GBP to 2 CHF.
 *** Survey conducted between September and October 2007 and report published in December 2007. This year's survey was conducted between November 2008 and January 2009.
 **** Findings of the Sixth Annual Deloitte Touche Tohmatsu (DTT) Global Financial Services Industry (GFSI) survey, published February 2009.

Figure 1: CB companies with a security strategy in 2007 and 2009



A year on and it's clear that most companies surveyed have taken initial steps by identifying a security manager and putting in place basic security protective measures, but they have not reached the level we see in other industries.

Mike Maddison, Head of UK Security & Privacy

Threats, vulnerabilities and impacts

Although the credit crunch made the most headlines in 2008, customer data loss has continued to feature in the news. The risk of customer data loss will always be a top security issue for consumer businesses as they focus heavily on developing a brand image and customer loyalty, both of which can be severely damaged because of an incident. In fact, survey results show that 83% of respondents perceive the most significant consequence of a data breach to be loss of reputation (see figure 2).

With phishing/pharming and social engineering attacks already affecting 39% of respondents, businesses should guard closely to prevent them directly involving their brand name. An increase in reputation-hijacking designed to abuse customer trust in a brand name for financial gain has been predicted for 2009. This type of attack increases potential damage to brand reputations and should be of particular concern to consumer businesses, especially in times of recession where there is already an increased likelihood that customers will switch brand.

The occurrence of external security breaches is increasing with 91% of respondents having experienced at least one in the past year.

Data on security breaches over the past year indicates that the occurrence of external security breaches is increasing with 91% of respondents having experienced at least one in the past year, compared with 64% in 2007. Internal security breaches were also common, affecting 76% of respondents. Virus outbreaks and employee misconduct were the most frequently experienced breaches, occurring for 35% and 43% of respondents, respectively. Notably, 61% are "not very" or only "somewhat" confident that their network is protected from internal breaches.

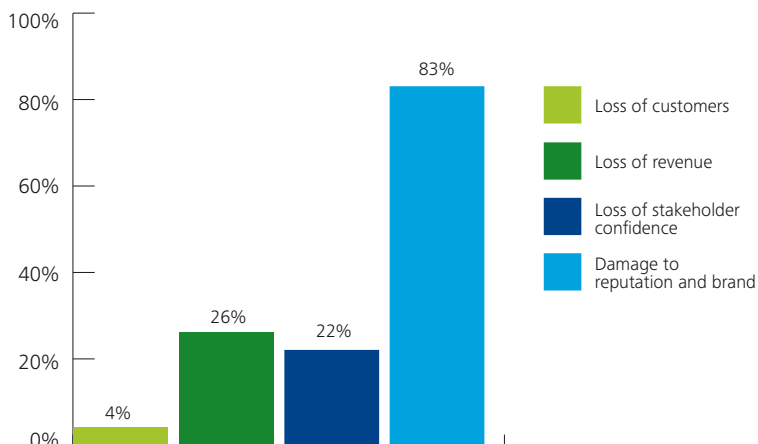
When asked about predictions for threats over the coming 12 months, respondents ranked social engineering, theft or leakage of customer data and employee misconduct as the greatest threats to their business. This is a dramatic change when compared with spyware, viruses/worms, and phishing/pharming predicted in 2007. The differences in the lists indicate that consumer businesses are beginning to recognise the evolution of security threats.



The perception that social engineering will be the top security threat for 2009 is consistent with security industry predictions that the technique will continue to be developed by hackers. Whilst the agreement between respondent and industry predictions shows an improved ability to look toward the future, survey results still suggest that consumer businesses are often failing to address security issues effectively. For example, employee training and awareness is an important method of protecting against social engineering attacks; however, two-thirds of respondents have not yet begun to develop a training programme.

As a direct result of the prominence of security breaches in the media, 73% of consumer businesses and 91% of retailers surveyed have undertaken activities to understand how they process customer data and how to improve the security around these processes. However, reduced budgets brought on by the recession will not aid security managers in addressing threats over the next 12 months.

Figure 2: Most severe consequences of data breaches



Third parties



Only 43% of respondents are performing periodic assessments after engagement with external parties. Of all respondents, 39% rely primarily on security clauses within contractual agreements to protect data provided to external parties.

The use of specialised suppliers can be both cost efficient and a means to deliver greater value to customers. While third parties can undoubtedly offer significant benefits, the use of an external supplier also introduces a host of additional security issues, especially where they are given access to sensitive customer data.

Survey results show that 96% of respondents use third parties that require access to customer information as part of their normal operation. This includes customer names, addresses, birth dates, health details and other data of a personal nature. Even when data is in the hands of a supplier, the originating company is still ultimately responsible, as shown by PCI DSS and DPA* requirements. They state that businesses should ensure that engaged third parties are capable, reliable and have sufficient controls in place to maintain the confidentiality and integrity of the data they are processing.

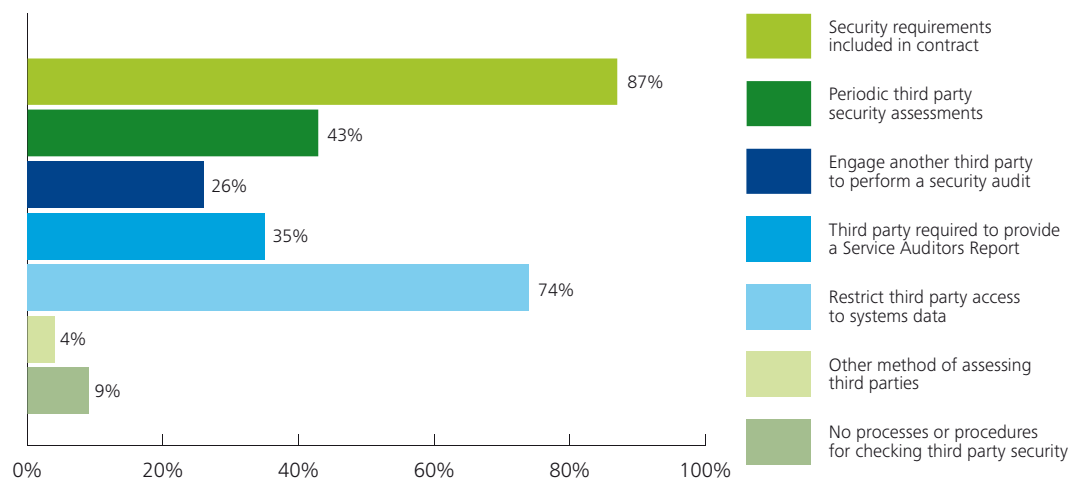
Although the percentage of respondents stating that they carry out security assessments before engaging third parties (74%) has doubled from last year's results (36%), only 43% are performing periodic assessments after engagement with external parties (see figure 3). Of all respondents, 39% rely primarily on security clauses within contractual agreements to protect data provided to external parties and, surprisingly, a further 9% of consumer businesses reported having no procedures in place to check third party security at all.

Additionally, it was found that 62% of respondents do not involve third parties in their business continuity plans. Suppliers are vital to ensuring the uninterrupted operation of consumer businesses, meaning that failing to include them in continuity plans increases vulnerability to supply chain and service disruptions with the worse case scenario resulting in the collapse of the business.

Now, more than ever, it is important that consumer businesses start taking third party security seriously. In an economic downturn, consumers tend to spend less, and some choose to trade down on brand quality but customers are not willing to compromise on data security: businesses need to find a way to cut costs and, as a result, may start to rely more heavily on third parties. Consumer businesses must not lose sight of the fact that they are ultimately responsible for the security of data collected from their customers. If a third party security breach results in the loss of customer data, the brand that customers trusted in the first instance will be the one to suffer the financial and reputational consequences.

*Payment Card Industry Data Security Standard (PCI DSS) and UK Data Protection Act (DPA) (1998)

Figure 3: Methods used to ensure that third parties provide adequate protection of information



Training and awareness

The growth in online business transactions, wireless network technologies and use of external memory devices to transport data provide many additional avenues where employee malpractice, intentional or otherwise, can occur. One way in which organisations can tackle these expanding security threats is through training their staff appropriately – both in complying with company policies and in reporting suspected security incidents.

Employee training and awareness programmes have not been defined by 74% of respondents. One-time training and ad hoc awareness sessions are provided by 54% of companies interviewed; however, to effectively change employee behaviours to increase security, defined and targeted training programmes are necessary.

Alarming, 14% of respondents do not provide employees with security training or awareness messages.

Of companies responding to the survey, 65% offer security training and awareness messages in the form of email or web alerts. Whilst shop floor staff often do not have access to web-based media, they do have access to card numbers and other sensitive data. In 70% of retail companies interviewed they don't receive training after inductions, although security training given during inductions (57%) is still the second most common method of education provided (see figure 4). Only 17% of respondents indicated that they provide instructor-led educational programmes.



The importance of training cannot be understated, particularly when considering its potential to reduce the number of security breaches. In fact, trained, security-minded staff would have the ability to quickly report or prevent and remediate all of the top six threats envisioned by survey respondents over the next 12 months, which include:

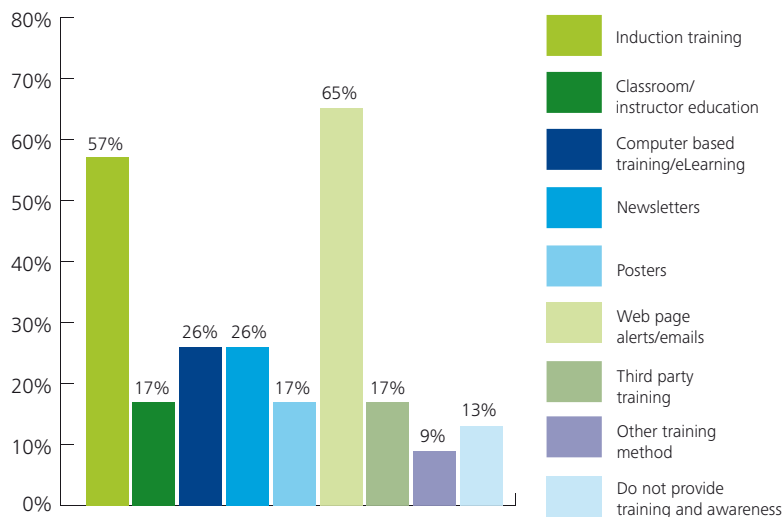
- Social engineering (3.0*)
- Theft or leakage of internal data (2.8*)
- Employee misconduct (2.8*)
- Virus/worm outbreaks (2.7*)
- Weak passwords (2.7*)
- Email attacks (average of 2.6*)

Employees trained in identifying these threats are a key first line of defence for enterprise security. However, 48% of survey respondents do not train their employees to identify and report suspicious activities. Inadequate detection leaves business operations vulnerable to threats, thereby risking company efficiency and profitability.

The survey results indicate that there are benefits to gain from the introduction or improvement of training and awareness schemes. Training programmes can be a cost effective way to improve security as well as to get additional benefit from previously implemented technology solutions. For example, training on secure data transfers could improve correct usage of encrypted transfer sites or email encryption software implemented in the past. To be effective, training and awareness schemes must provide employees with training tailored to their roles and responsibilities without inundating them with unnecessary information.

*Average score on a scale of 0 – 5, where 0 = non-threat and 5 = very high threat.

Figure 4: Methods of providing employee training and awareness



“Changing behaviours and embedding and understanding of security within the culture of the organisation is fundamental”

Mike Maddison, Head of UK Security & Privacy

Data quality

“With online transactional data and repositories growing more than 50% annually for most enterprises, data management challenges are also increasing.”

Why database archiving should be part of your DBMS strategy, quotation from a commissioned study conducted by Forrester Consulting on behalf of Clearpace, January 2008.

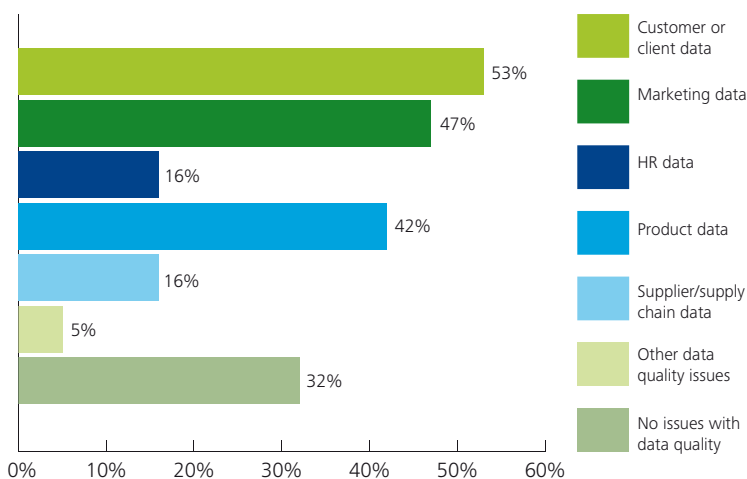
For consumer businesses, insights gained from the analysis of customer and sales data can be employed to gain a competitive advantage over rivals. Examples of innovative use of data by CB companies include product placement, targeted marketing and customer loyalty schemes. Conversely, following the ‘garbage in, garbage out’ principle, the use of incorrect or outdated information can be costly to businesses. Survey results indicate that identification and integrity of data are two common challenges facing consumer businesses.

In order to gain maximum value from their data, businesses must first identify it. Of the respondents, 74% have not performed an inventory of customer information to understand how their data is collected, stored and transmitted, although 39% are planning to do so within the next two years. Due to the falling cost of storing data, companies in the CB industry hold vast amounts of information, so finding customer or other

valuable data stores is often a major undertaking. However, the security implications of unidentified customer data should be of particular concern to consumer businesses as a breach could occur and go unnoticed.

Although consumer businesses are relatively adept at utilising the data they collect, our survey indicated significant room for improvement in the integrity of data. In fact, 63% of survey respondents said that they have experienced issues with data quality (see figure 5). Of those, 83% had issues specifically with customer data (53% of all respondents). Findings also show that only 14% and 10% of companies surveyed have data quality governance frameworks and data quality strategies, respectively. CB companies could better utilise the data they collect if they develop a strategy for identifying data and protecting its integrity.

Figure 5: Data quality issues



Conclusion

In 2009, funding problems caused by the economic downturn will have an affect over every aspect of security covered by the survey. In fact, budget and resource constraints were cited as a barrier to information security by 61% of respondents.

The key finding of the 2007 survey was that consumer businesses would benefit from taking a strategic approach to information security. On a positive note, results of this year's survey show that a number of consumer businesses have been working to develop defined strategies and governance frameworks over the past twelve months.

Companies making efforts to develop strategies and governance frameworks over the past year should see returns through increased ability to justify spending. They should also be in a better position to prioritise activities effectively and to continue security improvements, even with a decreased budget.

What can consumer businesses do to address security issues effectively over the year ahead?

- Revise security strategies to include plans for financial difficulties due to the expected economic situation, including business continuity plans spanning all third parties.
- Devise an approach to win funding, using metrics and reporting to demonstrate value of improved security to the business.
- Maintain reputation and customer trust. Businesses should not expose themselves to additional risks by failing to assess third parties or to address identified security threats.
- Look for "quick wins" in improving security. For example, training programmes can be relatively inexpensive to develop and offer big returns in improving security.
- Work to get more out of existing assets by developing a better understanding of data. This can increase profits and improve data integrity.



Authors

Katie Price
Andrew Vivian

Contributors

Nadine Sequeira

Designer

Jennie Atkinson

Contacts

Mike Maddison

Partner, Head of UK Security & Privacy

Email: mmaddison@deloitte.co.uk

Phone: 020 7303 0017

Andy Morris

Partner, UK Consumer Business Executive

Email: admorris@deloitte.co.uk

Phone: 020 7007 3308

www.deloitte.co.uk/security

Deloitte refers to one or more of Deloitte Touche Tohmatsu ('DTT'), a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTT and its member firms.

Deloitte LLP is the United Kingdom member firm of DTT.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© 2009 Deloitte LLP. All rights reserved.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Member of Deloitte Touche Tohmatsu