Financial Data at Risk in Development:
A Call for Data Masking in the U.K.

Sponsored by Informatica

Independently conducted by Ponemon Institute LLC

Publication Date: December 2010

Financial Data at Risk in Development:

Study of the Financial Services Industry in the United Kingdom

Part 1. Executive Summary

Worldwide access to online financial services by increasingly mobile consumers means development of applications to support online access to accounts and information through sophisticated mobile devices. New online applications hold the promise of making financial services organisations more attractive to their customers as well as more efficient, but risks associated with information security and data privacy remain the focus of regulators in an effort to protect consumers from identity fraud and other abuses of personally identifiable information (PII).

An overlooked privacy risk for financial services organisations is the vulnerability of personal and business information used for testing and application development.[1] As learned in previous Ponemon Institute research, it is during the test and development phase of new software applications that real data – including financial records, transactional records, and other personally identifiable information (PII) – is being used by as many as 80 percent of organisations. Further, test environments are less secure because data is exposed to a variety of unauthorized sources, including in-house testing staff, consultants, partners and offshore development personnel.

Previous Ponemon Institute research into how this situation affects the information security and privacy risks within the financial services industry were focused on U.S. based organisations[2], exposing lax practices and risk of non-compliance with numerous regulations. Intrigued, we sought to learn if financial services organisations in the UK faced similar information security and data privacy challenges as their contemporaries in the U.S. market. In the UK the regulatory environment is much different; instead of being subject to various state and federal mandates, banks in the UK are primarily directed by the Data Protection Act of 1998 as well as Basel I and II.

Another noteworthy difference between the U.S. and the UK is the approach each takes to privacy protection; in the U.S. regulations tend to focus on business processes, whereas in the UK (and throughout Europe) the focus is more broadly applied to protecting individuals.

Do these differences translate to differing attitudes toward data protection? Do they translate to different levels of risk? To answer these questions we surveyed 403 senior IT professionals in the financial services industry whose organisations have been engaged in application testing and development in order to better understand if the risk of using real data in development is being addressed. The results of that survey, underwritten by data integration software developer Informatica, are presented in the following report, *Financial Data at Risk in Development: A Call for Data Masking.*

We asked questions related to use of real data in the test and development process in the following categories:

- Types of real data used in application testing and development;
- Information security precautions and responsibilities;
- Use of cloud computing and outsourced services; and,
- Experience with data breaches involving real consumer data.

[1] See *Data Security in Development & Testing*, Ponemon Institute, August 31, 2009

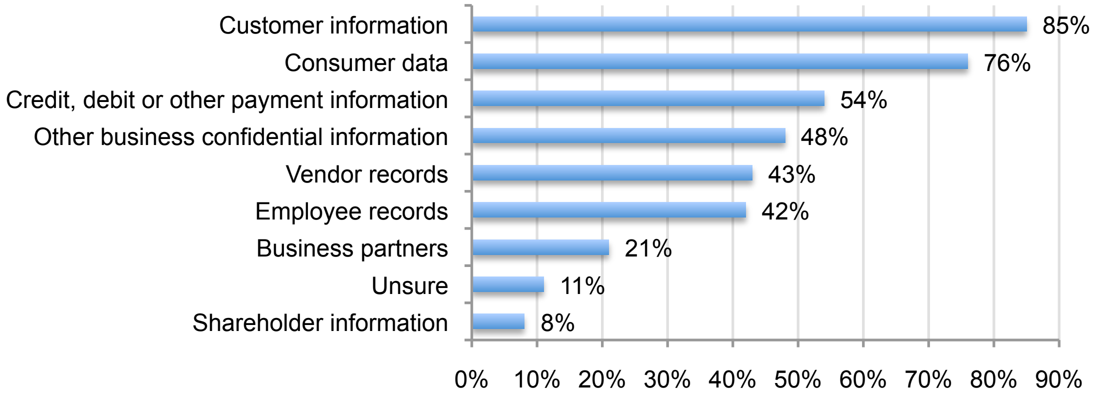
[2] See *Financial Data at Risk in Development: A Call for Data Masking*, Ponemon Institute, Oct 30, 2010

Part 2. Key Findings

According to the results of our study, it appears that the use of real data in development is putting sensitive financial and personally identifiable information at risk of exposure and data breach. Specifically, in this study we learned a number of important things about the use of real data in the test and development environment.

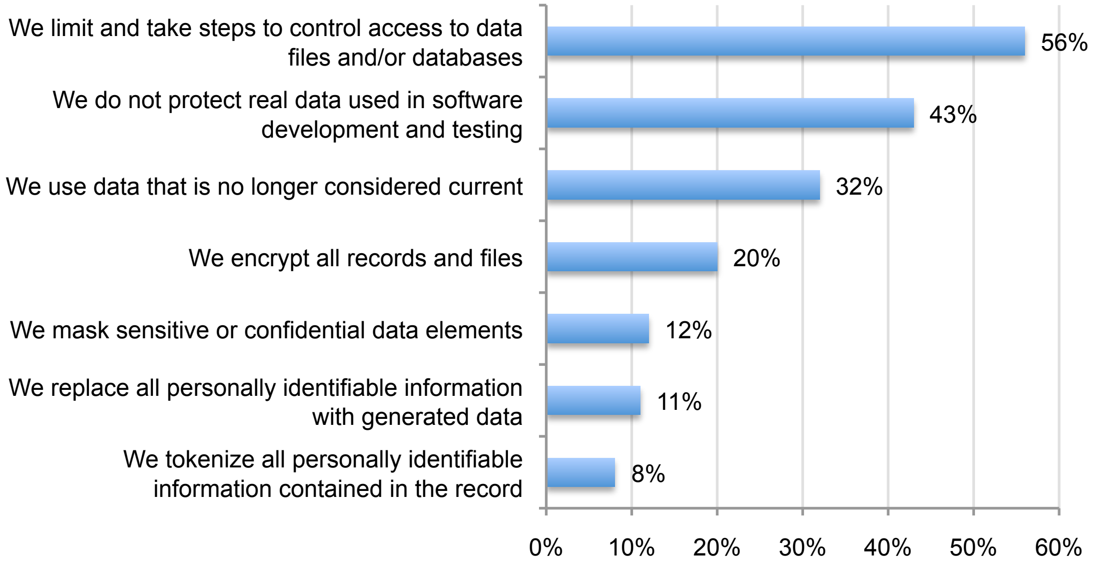
Real data used by financial services organisations for development and testing purposes is the most sensitive. According to Bar Chart 1, 85 percent of respondents' organisations use customer information, 76 percent use consumer data and 54 percent use credit, debit or other payment information. Forty-two percent say they use employee records and 48 percent say they use other business confidential information in development and testing operations.

Bar Chart 1: Real data used by financial service companies for development and testing
Each bar reflects the type of real data used for development or testing purposes



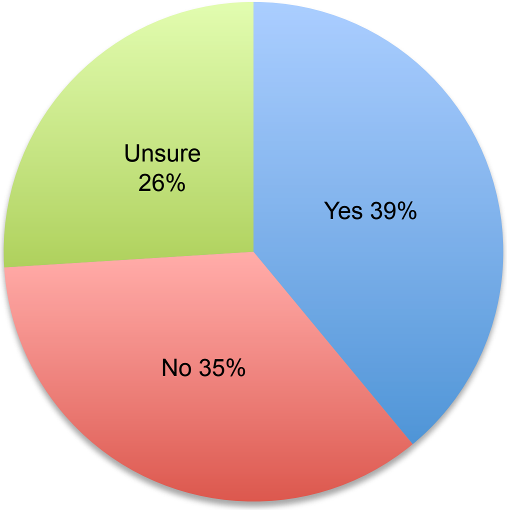
As shown above in Bar Chart 2, despite the sensitivity of the data, 45 percent do not protect real data used in software development and testing. Slightly more than half (56 percent) limit and take steps to control access to data files and/or databases.

Bar Chart 2: Steps taken to protect sensitive data in development and testing
Each bar reflects the steps taken to protect real data according to respondents



Many organisations admit real data used in the testing and development environment has been lost or stolen. Sixty-five percent of respondents say they have had a breach involving real data or are uncertain. The main consequence was disruption to business operations (87 percent) followed by 51 percent who say it reputation loss and 24 percent say it was lost revenues.

Pie Chart 1: Has real data used in the development and testing environment ever been lost or stolen?

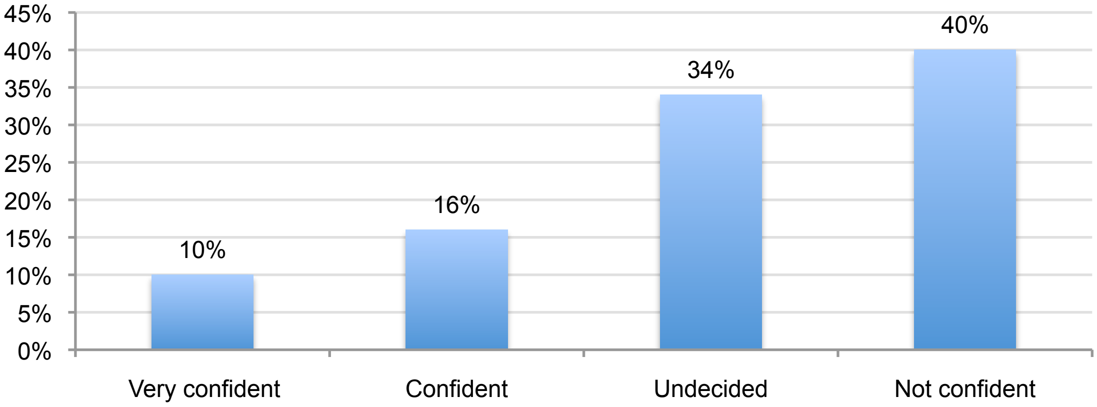


Q. If yes, what were the main consequences of the data loss or theft experienced by your organisation?

Table 1: Most salient consequences	**Pct%**
Disruption to business operations	87%
Reputation loss	51%
Revenue loss	24%
Customer turnover	13%
Regulatory action	6%
Other	2%

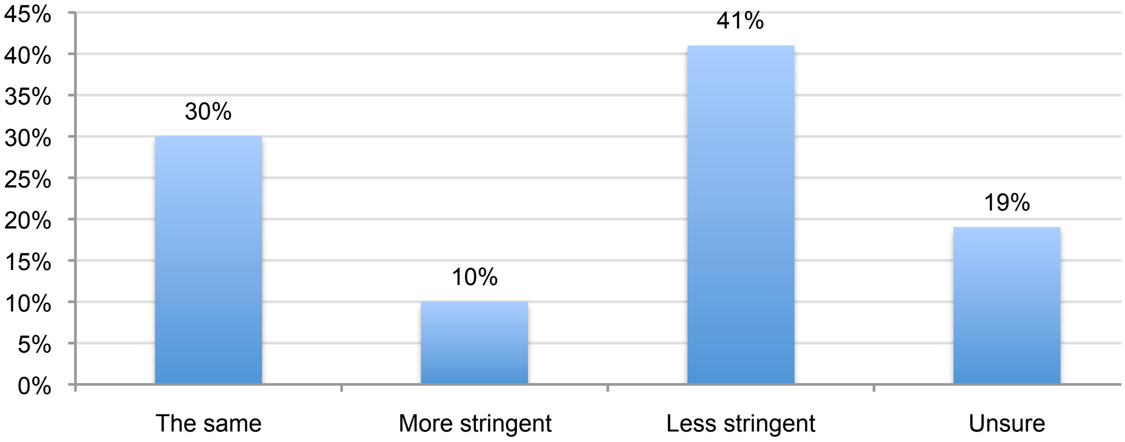
The majority of organisations would not know if sensitive data was lost or stolen. While 39 percent admit to losing real data in the testing and development environment, Bar Chart 3 shows that 40 percent of respondents are not confident that their organisation would be able to detect the unintentional loss or theft of real data and 34 percent are uncertain. This lack of confidence in the safeguarding of sensitive data jeopardizes customer trust and compliance.

Bar Chart 3: Respondents' confidence in their ability to detect data loss



Safeguards for financial data used for development and testing are not as stringent as they could be. Bar Chart 4 shows that only 10 percent of organisations report that they are using more stringent safeguards when protecting sensitive or confidential data in production than development. Almost half (41 percent) says their organisation uses less stringent safeguards when protecting sensitive or confidential data during test and development than when compared to production. Only 30 percent use the same safeguards when protecting sensitive or confidential data in both the production and development environments.

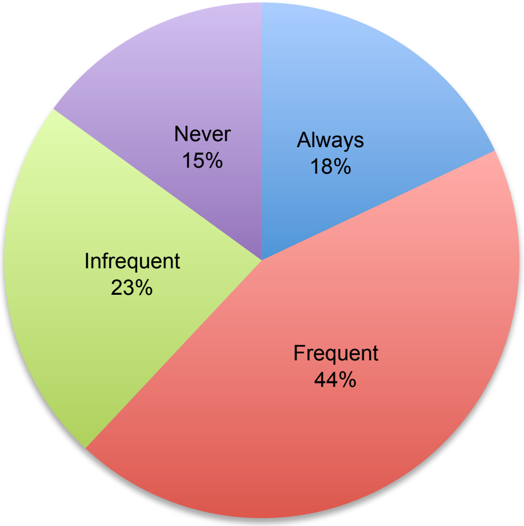
Bar Chart 4: Data security safeguards in development and production IT environments
Q. In comparison to safeguarding of sensitive or confidential data in a production environment, which statement best describes your protection of real data in the development and testing environment?



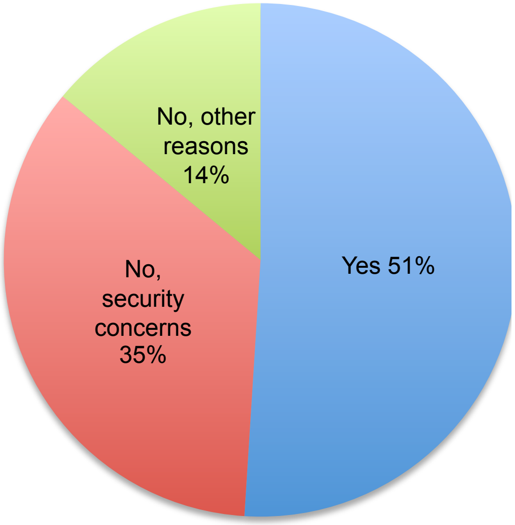
Outsourcing of real data can be risky. According to Pie Chart 2, 44 percent of organisations outsource the development and testing of software applications frequently. Another 18 percent of respondents say their organisations always outsource application development and testing.

As noted in Pie Chart 3, of those organisations that outsource, more than half (51 percent) say their organisations share real data. In contrast, 35 percent say they do not outsource because of security concerns. Clearly, without ensuring that third parties have appropriate safeguards in place, the organisation risks the loss or theft of real data.

Pie Chart 2: How often does your organisation outsource the development and testing of software applications?



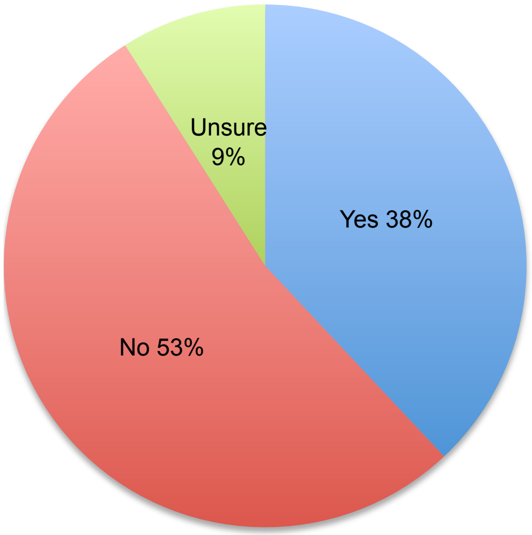
Pie Chart 3: Does the outsourcing relationship include the sharing of real data?



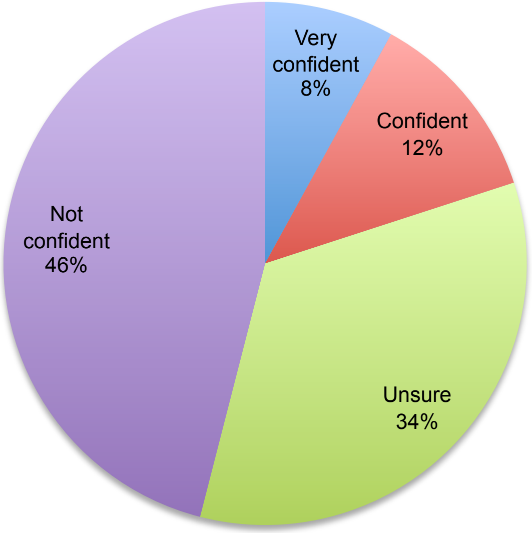
Cloud computing can be putting financial data at risk. According to Pie Chart 4, 38 percent of respondents say their organisations use public cloud infrastructure or platform services in the development and testing of software applications.

As shown in Pie Chart 5, of the organisations using cloud-computing resources for development and testing of software applications, 46 percent are not confident that the data housed in the cloud environment is safe and secure and 34 percent are undecided.

Pie Chart 4: Does your organisation utilize public cloud computing infrastructure or platform services in the development and testing of software applications?

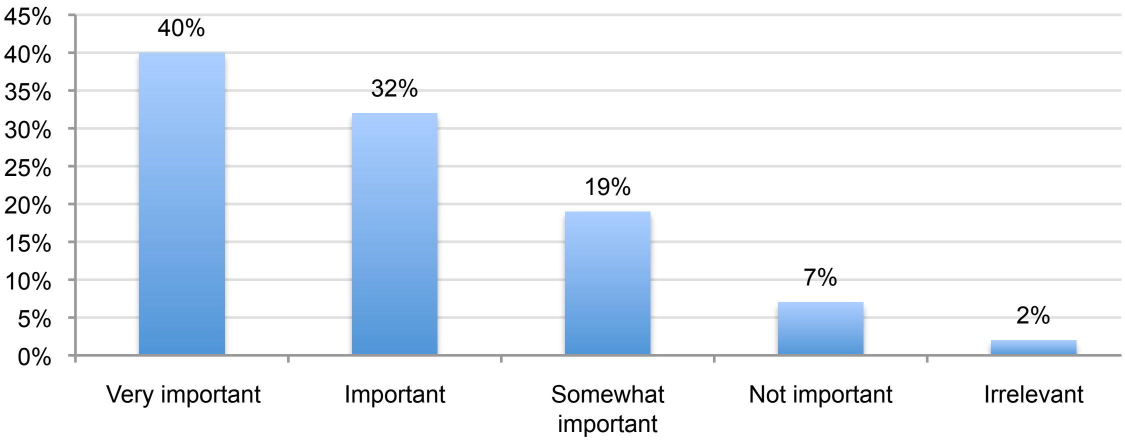


Pie Chart 5: How confident are you that data housed in the cloud environment is safe and secure?



Protection of financial data in the development and testing environment is important to respondents but most do not know or believe they are successful in achieving this goal. Bar Chart 5 shows 40 percent of respondents believe that meeting privacy and data protection requirements in the financial industry is very important and 32 percent believe it is important. Less than 9 percent see data protection activities as not important or irrelevant.

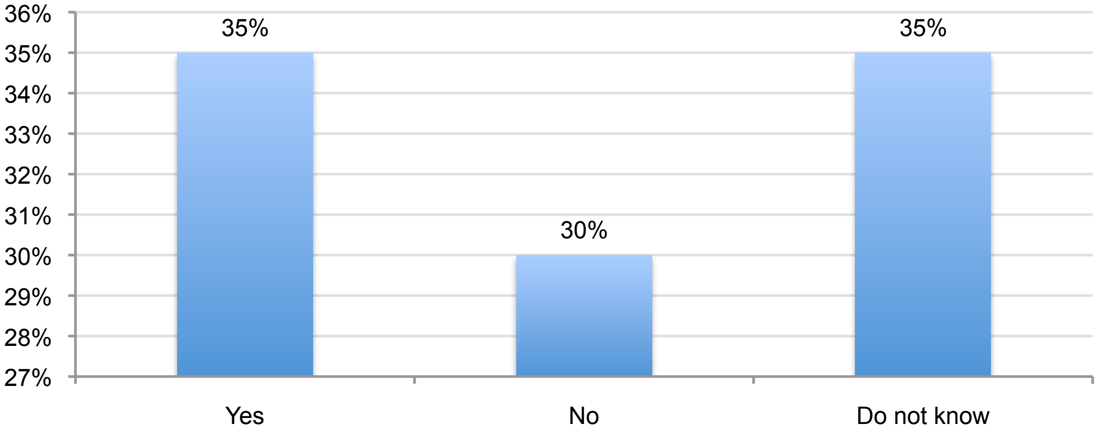
Bar Chart 5: How important is the protection of real data in development and testing?



Bar Chart 6 shows that 35 percent of respondents are unsure that their organisation is successful at protecting the privacy of consumers in the development and testing environment.

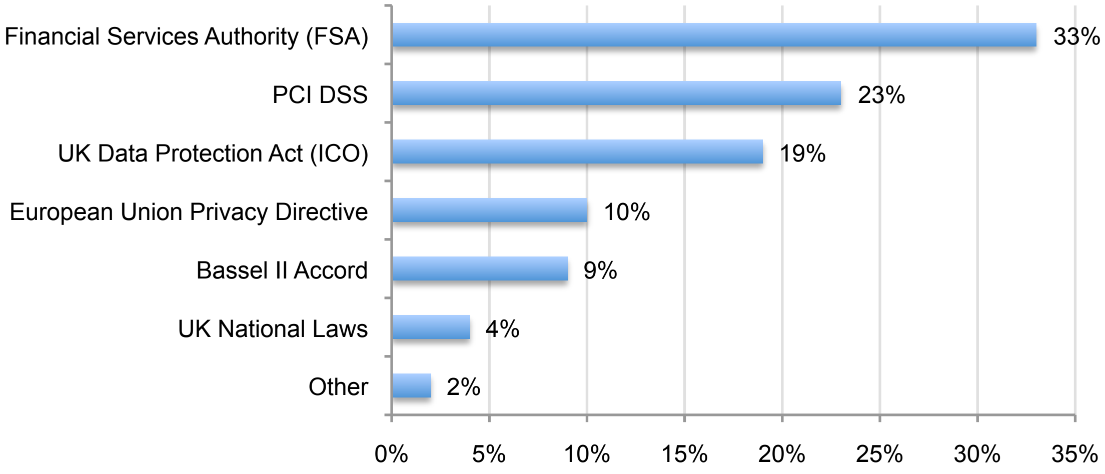
Another 30 percent believe their organisation is unsuccessful at protecting the privacy of consumers and customers in the development and testing IT environment.

Bar Chart 6: Is your financial services organisation successful at protecting customer privacy in the development and testing IT environment?



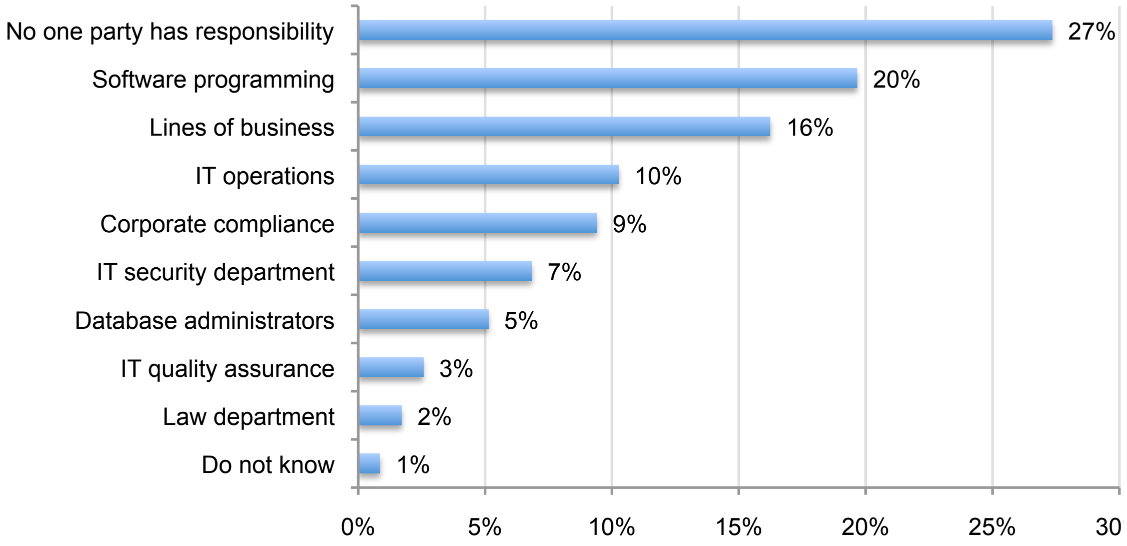
Respondents are concerned with the latest regulations affecting the financial services industry. According to Bar Chart 7, the regulations of greatest concern in meeting their privacy and data protection compliance requirements are Financial Services Authority (FSA) 33 percent, PCI DSS (23 percent,) UK Information Privacy Commission (ICO) 19 percent, European Union Privacy Directive 10 percent, and Basel II Accord 9 percent. Because only 35 percent are confident that they are successful in protecting customer privacy, these financial organisations risk non-compliance and costly fines if a data breach should occur.

Bar Chart 7: Regulations of greatest concern in meeting privacy and data protection compliance requirements



There is no clear accountability or responsibility for protecting real data in the testing and development environment among financial service organisations studied. Bar Chart 8 shows 27 percent say no one party has responsibility, 20 percent say software programming, followed by 16 percent who believe it is the lines of business that should ensure real data is protected. Only 7 percent believe it is IT security. This lack of governance and risk management of sensitive test information is increasing the possibility of a breach. As we discussed above, test environments can be less secure for a variety of reasons.

Bar Chart 8: Who in the financial services organisation is most responsible for protecting real data in the development and testing IT environment?



Part 3. Implications for financial services and recommendations

Ponemon Institute believes that data protection is more difficult and more costly, with a greater risk of non-compliance and lost customer trust, when there is a lack of accountability for the protection of sensitive information, including data used in testing and development. Twenty-seven percent of organisations in this study report no one person or department with responsibility for the protection of real data during application testing and development. This number is surprisingly high for organisations in a highly regulated industry such as financial services.

Previous Ponemon Institute research has found that giving executive-level authority for information security to a chief information security officer (CISO) or equivalent role is vital to the development and execution of successful information security programs. As reported in the *2009 UK Cost of a Data Breach Study*, the presence of a CISO benefits organisations through fewer data breach incidents as well as lower costs when a data breach occurs.[3]

This lack of oversight may play a role in other results from this study pointing to increased information security risk, including:

- High rates of real data used in software testing and development;
- Lack of protective measures used to secure real data during software testing and development; and,
- Lack of confidence in the organisation's ability to protect real data during software testing and development.

The types of real data used in software testing and development, such as customer information, credit/debit payment information, and employee records, are examples of high-value, personally identifiable information (PII) used to perpetrate crimes associated with identity fraud. Protecting PII should be a priority for any organisation at all times, yet our research shows that 43 percent of organisations surveyed take no steps to do so.

Furthermore, many organisations in our study report unknown or less stringent information security measures compared to the organisation's typical security posture (29 percent), and a significant lack of confidence (40 percent) in their organisation's ability to protect real data used for testing and development. Such lack of concern for security puts financial services organisations at risk for being in non-compliance with various laws, regulations, and standards that apply, including some of those identified as among the most concerning, among others:

Data Protection Act of 1998 – Provides definitions, guidance and requirements for the collection, use, management, and security of personally identifiable information by commercial organisations. Serves as the UK's implementation of the EU Data Protection Directive of 1995 outlining protections for sensitive personal data and privacy.

Basel II – Non-compliance with Basel II security guidelines is penalized through higher business costs associated with greater required capital reserves and higher costs for access to capital markets.

PCI DSS – The Payment Card Industry Digital Security Standard is an industry-defined standard for protecting data vital in transactions involving payment cards such as debit and credit cards.

For those organisations reporting a point of accountability, only a small number says this responsibility lies with their organisation's compliance department (9 percent) or legal office (2 percent). None of the organisations surveyed reports that the privacy officer or department has oversight.

[3] 2009 UK Cost of Data Breach Study, Ponemon Institute January 2010.

Instead, the vast majority of organisations say responsibility for information security in test and development environments is at the business level (16 percent) or within various IT functions (20 percent combined).

This finding suggests that security decision-making may be motivated more by achieving business objectives than by addressing data security risks through compliance and the application of best security practices. Such decisions may include the use of outsourcing (85 percent) and cloud computing services (38 percent) by a large number of financial services organisations to facilitate application testing and development in spite of a lack of confidence in data security in these processes. This also suggests that the cost-saving advantages of these services may be taking precedence over security considerations.

These services should not be discouraged. However, given the potential for heavy fines and penalties, customer churn, reputational damage, and the overall costs associated with a data breach, it is recommended that financial services organisations proceed with great caution before outsourcing to third parties. This should include a vigorous evaluation of any prospective partner's security policies and procedures, and with detailed contractual provisions to further ensure information security remains a priority throughout the process.

On a positive note, investments in technologies, processes, policies, and personnel under the guidance of an information security strategy are recommended in order to reduce an organisation's risk profile. We recommend the following:

- Assign a single point of responsibility (CISO or equivalent) for the safeguarding of real data used in application testing and development;

- Develop security policies for the protection of real data used in application testing and development;

- Implement employee training and awareness programs;

- Use encryption, data leak prevention, access management, and other information security technologies; and,

- Use de-identified, masked, or dummy data rather than live data in the test and development process.

These technology tools can transform or mask sensitive or confidential data without diminishing the richness of the data necessary to successful testing and development. When making this investment, we recommend you consider the following features: sensitive field and table relationship discovery, comprehensive set of masking rules, masking policies, extensive database connectivity, reporting and auditing and scalability.

Part 4. Methods

One national sampling frame consisting of nearly 8,000 IT or IT security practitioners who work for financial service organisations in the United Kingdom was used to recruit participants to this survey. Our omnibus sampling frame was built from several proprietary lists of experienced IT and IT security practitioners. In total, 602 respondents completed the survey. Of the returned instruments, 28 surveys failed reliability checks. A total of 442 surveys were used as our final sample, which represents a 5.6 percent response rate. One screening question about the use of real data in the development and testing reduced the final sample to 403 respondents.

Table 2: Sample response	Pct%
Total sampling frame	7901
Bounce-back	483
Total returns	470
Rejected returns	28
Final sample	442
Response rate	5.6%
Final sample after screening	403

Pie Chart 6 summarizes the respondents' companies by segment in the financial services industry. The largest segment (31 percent) includes retail banking, which includes building societies. The second largest segment (19%) includes payment-processing companies. sixteen percent of respondents are employed by insurance companies.

Pie Chart 6: Industry segment for participating healthcare organisations

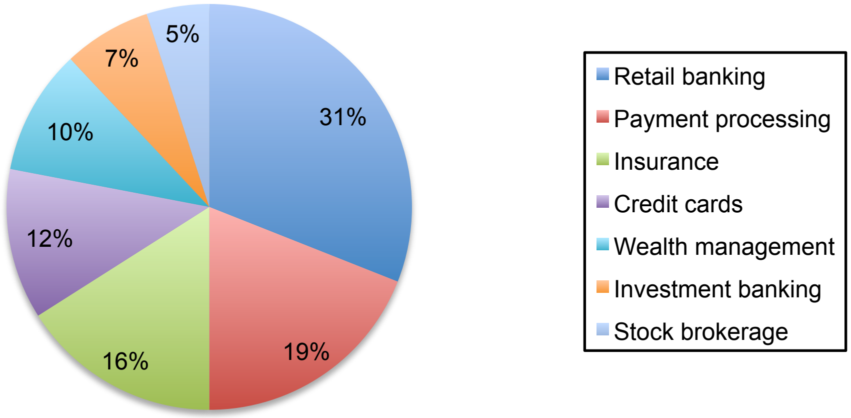


Table 3 reports the organisation's headcount. More than 41 percent of respondents are located in larger-sized companies with more than 5,000 employees.

Table 3: The worldwide headcount of respondents' financial services organisations	Pct%
Less than 500	11%
500 to 1,000	16%
1,001 to 5,000	32%
5,001 to 25,000	21%
25,001 to 75,000	10%
More than 75,000	10%
Total	100%

Table 4 reports the respondents' primary functions. Respondents hold, on average, 10.9 years of overall work experience and 9.0 years in IT or IT security fields. The total years in current position is 5.1 years on average.

Table 4: Primary job functions of respondents in financial services organisations.	Pct%
IT operations	30%
Programming	26%
Testing	12%
Quality assurance	5%
Compliance	7%
IT security	13%
Security	3%
Risk management	4%
Other	0%
Total	100%

Table 5 reports the respondents' position level. As can be seen, a majority of respondents self-report their positions at or above the supervisory level.

Table 5: Respondents' organisational level in healthcare organisations	Pct%
Senior executive	3%
Vice president	1%
Director	15%
Manager	26%
Supervisor	15%
Analyst or technician	25%
Associate or staff	11%
Contractor	3%
Other	1%
Total	100%

Part 5. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners located in the UK. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used an omnibus collection method, it is possible that other items contained in the Meta survey instrument bias responses.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Appendix: Survey Question Details

Fieldwork concluded on November 15, 2010

Q1. Does your organisation use real data for the following purposes? Check all that apply:	Percentage
Software development	88%
Testing of applications	79%
Production support	46%
Training	13%
Other	3%
No, my organisation does not use real data outside the production environment (Stop)	8%
Number of respondents saying no	39
Revised sample size	403

Q2. What types of real data do you use for development and testing purposes? Please check all that apply. **(More than one response allowed)**	Pct%
Customer information	85%
Employee records	42%
Consumer data	76%
Credit, debit or other payment information	54%
Vendor records	43%
Shareholder information	8%
Business partners	21%
Other business confidential information	48%
Unsure	11%
Total	388%

Q3. What precautions does your organisation take to protect real data during the development and testing process? Please check all that apply. **(More than one response allowed)**	Pct%
We mask sensitive or confidential data elements	12%
We tokenize all personally identifiable information contained in the record	8%
We limit and take steps to control access to data files and/or databases	56%
We replace all personally identifiable information with generated data	11%
We encrypt all records and files	20%
We use data that is no longer considered current (i.e., older data files)	32%
We **do not** protect real data used in software development and testing	43%
Total	182%

Q4. In comparison to your organisation's safeguarding of sensitive or confidential data in a production environment, which statement best describes your protection of real data used in the development and testing environment?	Pct%
My organisation uses the **same** safeguards when protecting sensitive or confidential data in both the production and development environment.	30%
My organisation uses **less stringent** safeguards when protecting sensitive or confidential data in the development environment.	41%
My organisation uses **more stringent** safeguards when protecting sensitive or confidential data in the development environment.	10%
Cannot determine	19%
Total	100%

Q5. How confident are you that your organisation will be able to detect the unintentional loss or theft of real data in the development and testing environment?	Pct%
Very confident	10%
Confident	16%
Undecided	34%
Not confident	40%
Total	100%

Q6a. How often does your organisation outsource the development and testing of software applications?	Pct%
Always	18%
Frequently	44%
Infrequently	23%
Never (Go To Q7)	15%
Total	100%

Q6b. Does the outsourcing relationship include the sharing of real data?	Pct%
Yes	51%
No, because of security concerns	35%
No, other reasons	14%
Total	100%

Q7a. Does your organisation utilize public cloud computing infrastructure or platform services in the development and testing of software applications?	Pct%
Yes	38%
No	53%
Don’t know	9%
Total	100%

Q7b. If yes, how confident are you that data housed in the cloud environment is safe and secure?	Pct%
Very confident	8%
Confident	12%
Undecided	34%
Not confident	46%
Total	100%

Q8. Who in your organisation is most responsible for protecting real data in the development and testing environment? Please check only one responsible party.	Pct%
Lines of business	16%
Software programming	20%
Database administrators	5%
IT operations	10%
IT quality assurance	3%
IT security department	7%
Privacy office	0%
Corporate compliance	9%
Law department	2%
No one party has responsibility	27%
Do not know	1%
Total	100%

Q9a. Has real data used in the development and testing environment ever been lost or stolen?	Pct%
Yes	39%
No	35%
Unsure	26%
Total	100%

Q9b. If yes, what were the main consequences of the data loss or theft experienced by your organisation? Please check the top three choices.	Pct%
Customer turnover	13%
Revenue loss	24%
Regulatory action	6%
Lawsuits	0%
Reputation loss	51%
Disruption to business operations	87%
Other (please specify)	2%
Total	183%

Q10. With respect to meeting privacy and data protection requirements in the financial services industry, how important is the protection of real data in the development and testing environment.	Pct%
Very important	40%
Important	32%
Somewhat important	19%
Not important	7%
Irrelevant	2%
Total	100%

Q11. What regulations are of greatest concern to you and your organisation in meeting privacy and data protection compliance requirements? Please check the top two choices.	Pct%
UK Data Protection Directive	4%
PCI DSS	23%
UK Information Privacy Commission (ICO)	19%
European Union Privacy Directive	10%
Financial Services Authority (FSA)	33%
Bassel II Accord	9%
Other	2%
Total	100%

Q12. In your opinion, do you believe your company is successful at protecting customer privacy in the development and testing environment?	Pct%
Yes	35%
No	30%
Do not know	35%
Total	100%

Your role & organisation	
What organisational level best describes your current position?	Pct%
Senior executive	3%
Vice president	1%
Director	15%
Manager	26%
Supervisor	15%
Analyst or technician	25%
Associate or staff	11%
Contractor	3%
Other (please specify)	1%
Total	100%

Check the **Primary Function** where you reside within your organisation.	Pct%
IT operations	30%
Programming	26%
Testing	12%
Quality assurance	5%
Compliance	7%
IT security	13%
Security	3%
Risk management	4%
Total	100%

Experience in years	Mean
Total years of overall work experience	10.9
Total years in IT or security fields	9.01
Total years in current position	5.08

What best describes your organisation?	Pct%
Retail banking	31%
Credit card	19%
Insurance	16%
Payment processing	12%
Wealth management	10%
Investment banking	7%
Stock brokerage	5%
Total	100%

What is the worldwide headcount of your financial services organisation?	Pct%
Less than 500	11%
500 to 1,000	16%
1,001 to 5,000	32%
5,001 to 25,000	21%
25,001 to 75,000	10%
More than 75,000	10%
Total	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organisations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.