

Sponsored by



Independently Conducted by



Presents

2008 Study on the Uncertainty of Data Breach Detection

Report of IT Practitioners in the
UK, Germany & France

Published by Ponemon Institute LLC

August 5, 2008

Private & Confidential Document. Please Do Not Quote Without Express Permission.

2008 Study on the Uncertainty of Data Breach Detection

Report of IT Practitioners in the UK, Germany & France

Executive Summary by Dr. Larry Ponemon, August 5, 2008

Mainframe data security has become a critical IT issue. Typically, organizations address this risk by locking down applications to keep unauthorized outside users from accessing them. What this approach does not address is the threat of the negligent or malicious insider who is authorized to access an organization's sensitive information. Research has shown that the biggest data security threat organizations face is internal—both negligent and malicious.

In a case of insider negligence, the British government last year lost the details of 25 million people on two computer discs. The personal information included names, dates of birth, addresses, child benefit and national insurance numbers of adults and children and bank account details. More than seven million families were affected.

According to the reports, in October 2007 a clerk downloaded the entire child benefit database at the Revenue and Customs office and sent it via courier to the audit office in London. Downloading the database broke department rules. Further, the password-protected discs weren't sent by recorded or registered delivery.

Nationwide, the UK's largest building society, lost customers' personal data when an employee's laptop was stolen in a domestic burglary in August 2006. The employee dutifully reported its loss and then went on holiday. However, it took three weeks for Nationwide to realize that the laptop contained confidential customer information. This failure to take proper steps to investigate the data breach cost Nationwide £1m in fines following an investigation by the Financial Services Authority (FSA).

Compuware Corporation and Ponemon Institute, LLC are pleased to report the results of the *2008 Study on the Uncertainty of Data Breach Detection in the UK, Germany and France*. The purpose of this study is to understand how organizations in these countries detect a data breach and then gather all the facts to make informed decisions about how to respond to the incident. According to many of the respondents in these three countries, their organizations have had data breaches caused by negligent insiders and a significant number have been caused by malicious insiders.

We surveyed more than 2,484 IT practitioners in the UK, Germany and France who have significant experience in IT operations and security and are employed in a variety of industries. Key demographics for survey respondents are summarized at the conclusion of this report.

Survey questions addressed the following issues:

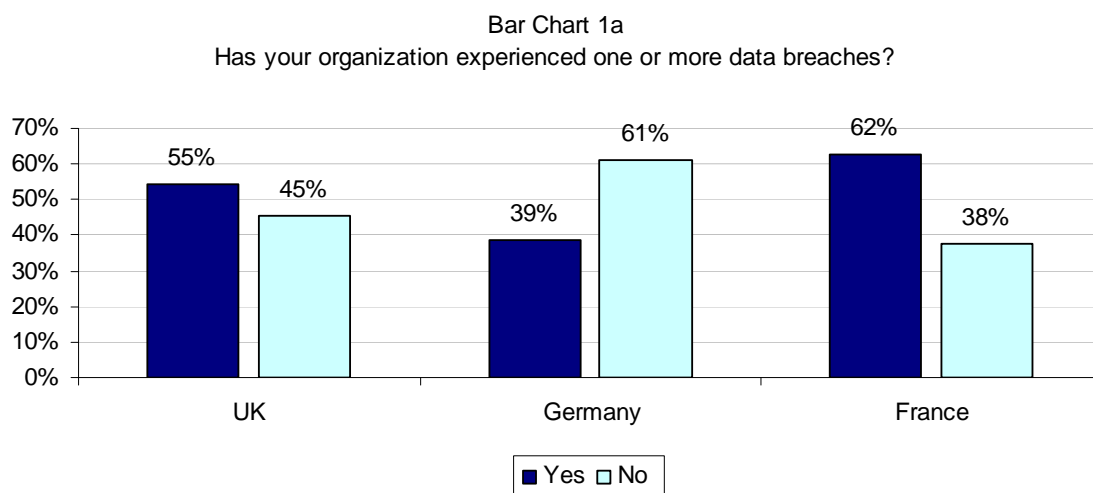
- What do IT practitioners believe are the most likely causes of data breaches in their organizations?
- Was the organization able to determine the root cause of the data breach?
- How did the organization obtain facts about the data breach?
- What facts are most important to understanding the cause of the breach?
- What tools or techniques were used to determine the cause of the breach?
- What tools do organizations need to deter breaches?
- Who is accountable for detecting and responding to a breach?

Key Findings

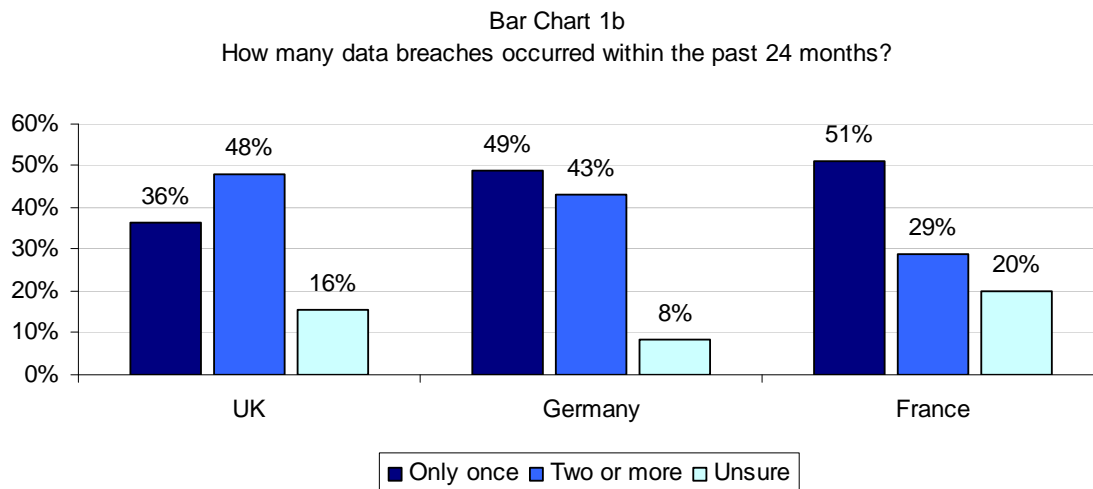
Following are the most salient findings from the study are presented below. Please note that most of the results are displayed in bar chart format. The actual data utilized in each graph and referenced in the paper can be found in the percentage frequency tables attached as the Appendix to this paper.

A majority of organizations in the UK, Germany and France have had a data breach, and many have had more than one.

As shown in Bar Chart 1a, the majority of IT practitioners in the UK (55%) and France (62%) report that their organization has experienced one or more data breaches involving the loss or theft of information about individuals such as consumer data, customer information, employee records, and so forth. Germany has a lower incidence of data breaches, with only 39% of respondents reporting a data breach in their organization.



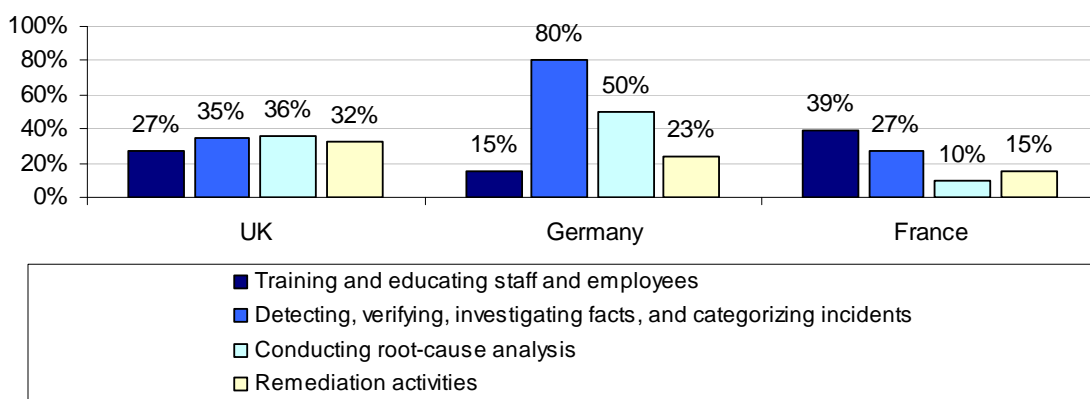
As shown in Bar Chart 1b, there is a higher incidence of two or more data breaches in the UK and Germany (48% and 43% respectively). In France, only 29% report multiple data breaches. There is also greater uncertainty about the number of data breaches among respondents in France and the UK.



IT practitioners are involved in many different activities related to data breach detection and response.

Bar Chart 2 shows the top four activities IT practitioners are typically involved in when their organizations have a data breach. These activities include: training and educating staff and employees; detecting, verifying, investigating facts and categorizing incidents; conducting root-cause analysis; and remediation activities. In Germany, an overwhelming majority (80%) are involved in detecting, verifying, investigating and categorizing incidents. In France, 39% of respondents are involved in training and education. In the UK, the respondents are involved in conducting root-cause analysis.

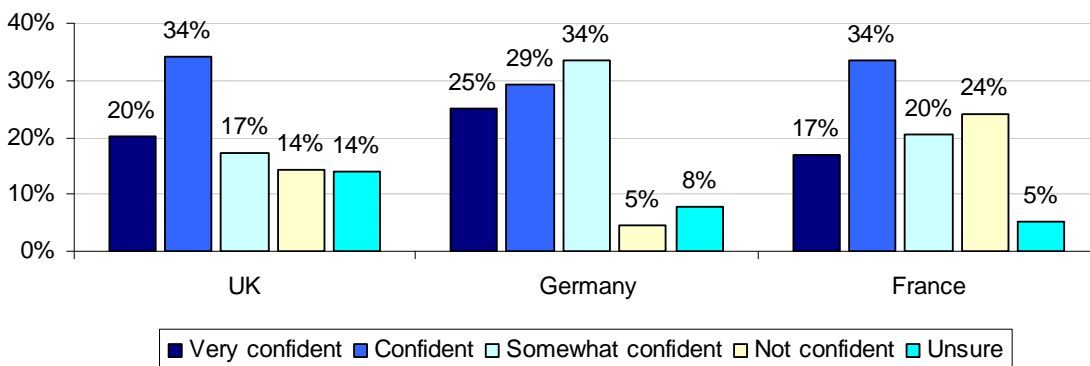
Bar Chart 2
How were you involved? Top four answers.



The majority of IT practitioners seem to be very confident or confident about their organization’s ability to detect the loss or theft of sensitive or confidential information.

When asked how confident they are that all data breaches involving the loss or theft of personal information will be detected, 54% of respondents in both the UK and Germany and 51% from France indicate that that are very confident or confident (Bar Chart 3). In Germany, only 13% are not confident or unsure, whereas 28% from the UK and 29% from France are not confident or unsure.

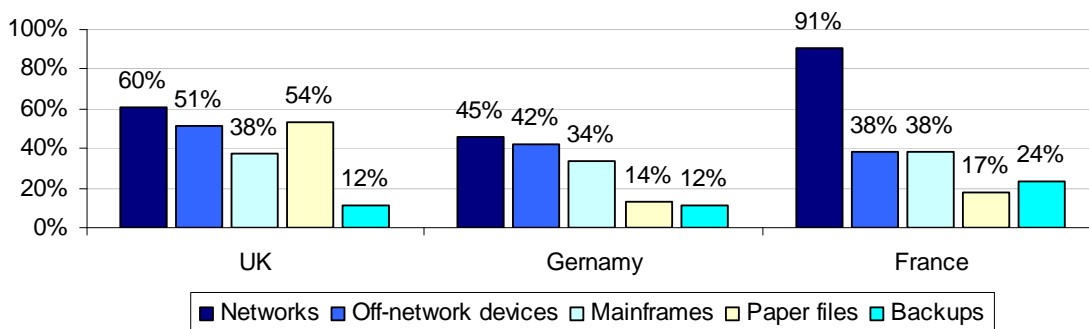
Bar Chart 3
How confident are you that all data breaches involving the loss or theft of personal information will be detected within your organization?



The cause of data breaches and the IT environment where data breaches occur are linked.

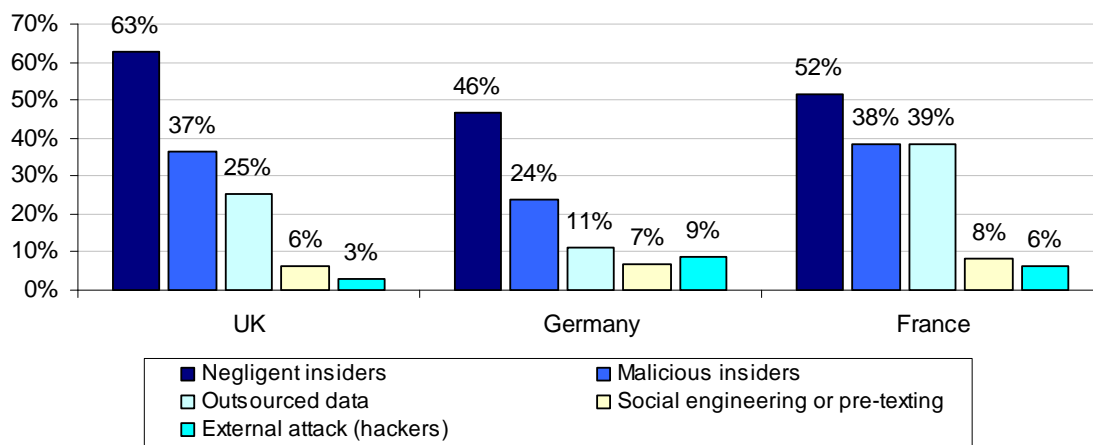
Organizations motivated to prevent data breaches should assess the risk posed by potentially negligent or malicious employees with access to their networks or who have sensitive information on off-network devices. According to Bar Chart 4, IT practitioners report that networks and off-network devices are most vulnerable to a data breach, followed by mainframes. The only exception to this is in the UK where paper files (54%) are considered more vulnerable than off-network devices (51%) and the mainframe (38%).

Bar Chart 4
IT environment where data breached occur



Negligent insiders, malicious insiders and outsourced data to third parties are the top three causes of a data breach (Bar Chart 5). As more employees are allowed to remotely access their organizations' networks or use off-network devices containing confidential data while traveling or working from other locations, the risk to sensitive and confidential data increases. Paper documents containing customers and employees personally identifiable information also pose a risk when in the hands of negligent or malicious insiders.

Bar Chart 5
What are the most likely causes of data breach?



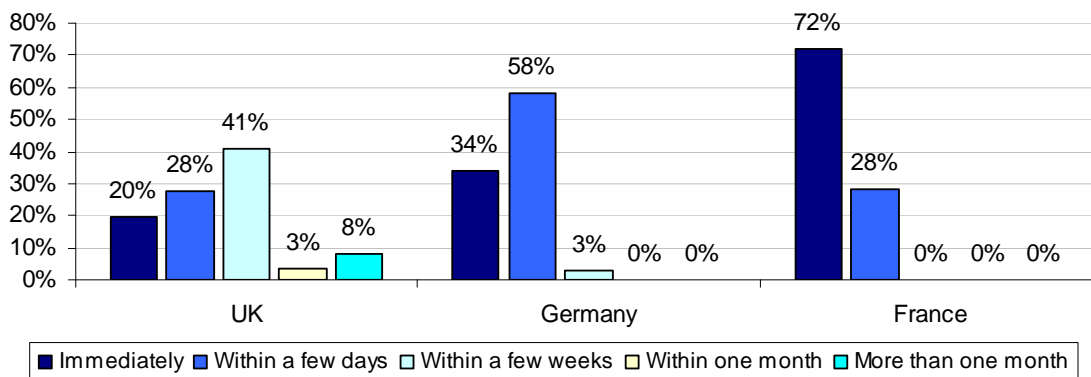
Notification of victims is considered important and generally occurs within a few days.

Most respondents in the UK, Germany and France notify victims immediately or within a few days (Bar Chart 6). The UK has the highest rate of notification, with 19% of participants in the study

reporting that the data breach incident required the organization to notify possible victims after the event (as required by the FSA). Only 9% of respondents from Germany and 5% of respondents from France were required to notify the victims.

However, Germans and French consider quick notification to be more important than those from the UK. Ninety percent of Germans and 84% of French respondents consider quick notification important or important as compared to 69% of UK respondents.

Bar Chart 6
How long after discovering the data breach are victims notified?

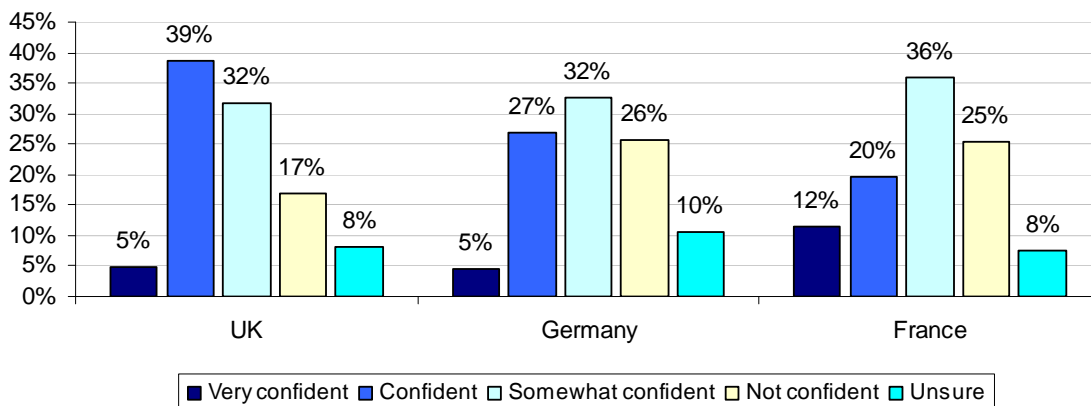


IT practitioners are somewhat confident of their ability to learn all the facts about the data breach.

It's very important to understand not only how a breach occurred, but also to be able to take the necessary steps so the breach doesn't occur again. The majority of respondents (85% in the UK, 70% in Germany and 65% in France) state that they were able to determine relevant facts—that is the “who, what, where, when and how”—to pinpoint the root cause of the incident as well as who needs to be notified.

However, respondents are less confident that they can obtain all of the facts associated with the breach; the breakdown by country is shown in Bar Chart 7. Forty-four percent of respondents from the UK, 32% from Germany and 32% from France indicate that they are very confident or confident about their organization's ability to determine root causes of the breach incident.

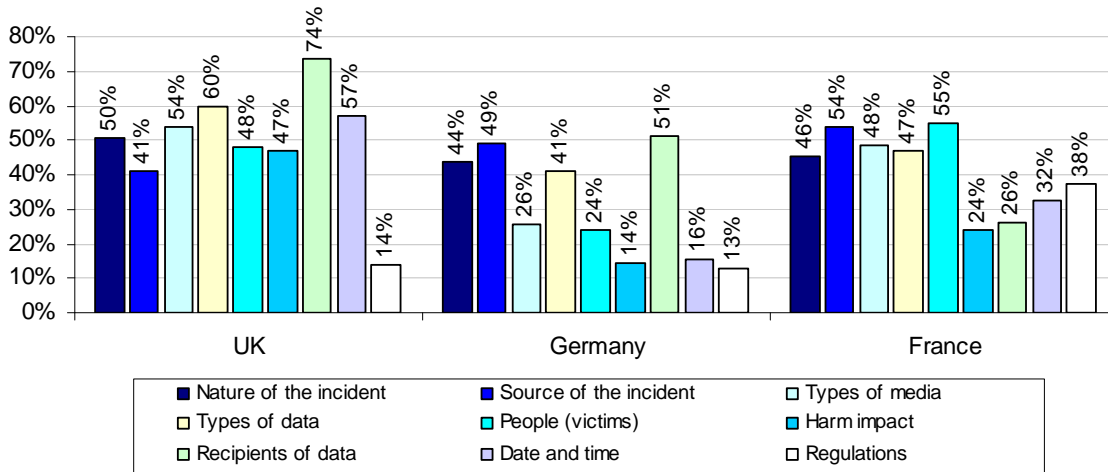
Bar Chart 7
How confident are you that all the facts about the breach have been obtained?



Types of information and media lost or stolen are key to understanding the data breach.

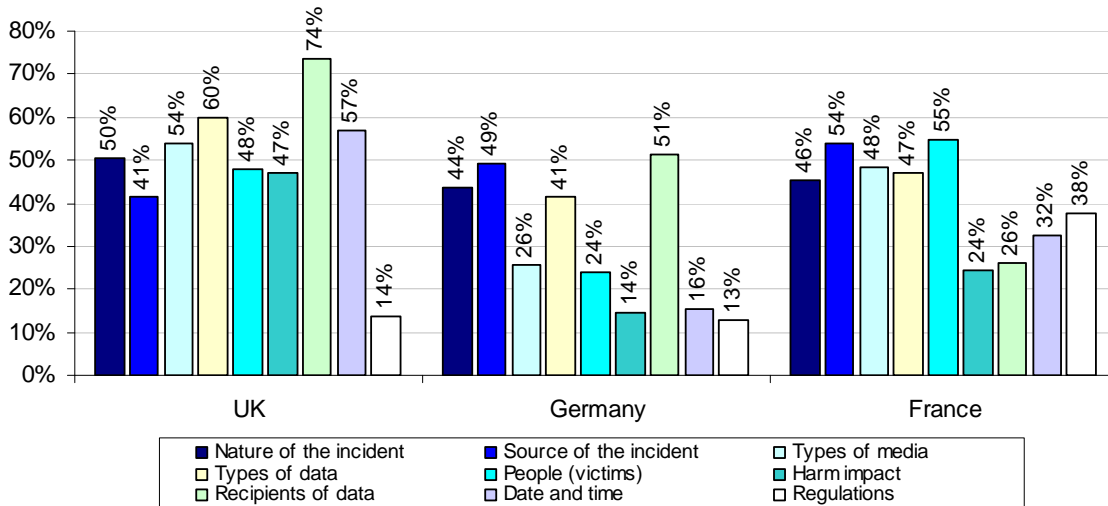
In Bar Chart 8, IT practitioners cite the following the following as the top four facts gathered to detect and respond to data breach incidents: types of information lost or stolen, types of media (e.g. files or data-bearing electronic devices lost or stolen), source of the incident (i.e. privileged users, general employees, contractors and/or IT glitches that caused the event), and date and time of the actual incident. The exception to this is that the UK respondents most commonly gathered information about the people whose information was lost or stolen (74%). This could be due to the fact that they have the highest rate of customer notification.

Bar Chart 8
 What facts were gathered to detect and respond to the incident?
 More than one response is permitted



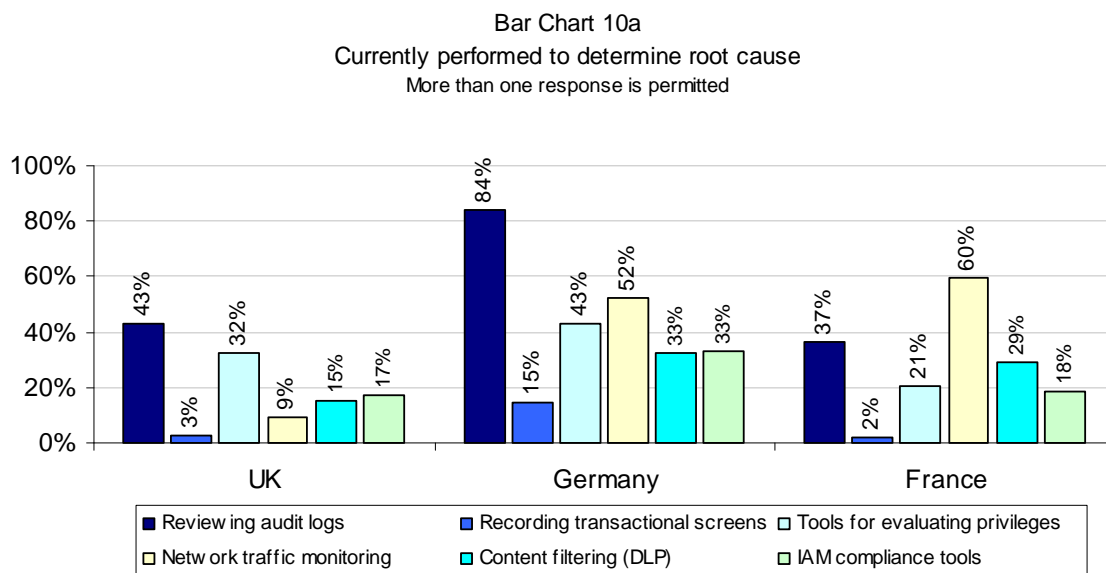
However, as noted in Bar Chart 9, when asked which facts are most important (i.e., very important or important) to understanding root causes, this varies across countries. In the UK, respondents indicate that recipients and types of data are the most useful. German IT practitioners believe that recipients of the data and the source of the incident are the most helpful. And in France, people (i.e. the victims) and the source of the incident are the most important.

Bar Chart 9
 Very important or important to understanding the cause of the data breach incident
 More than one response is permitted

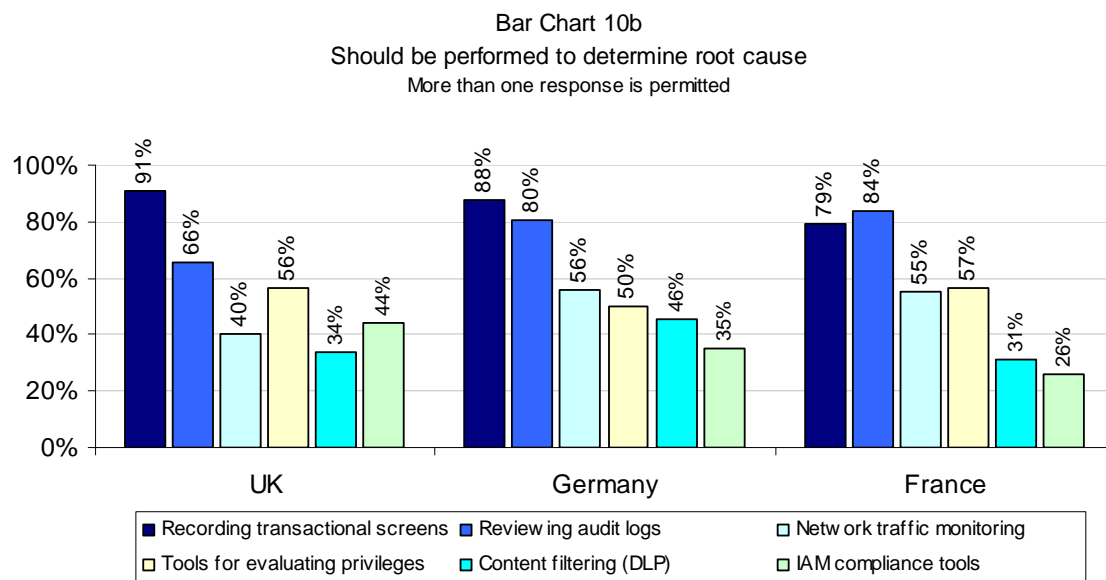


IT practitioners indicate that recording transactional screens and reviewing audit logs would be the most useful ways to obtain facts about the data breach and deter future breaches.

As shown in Bar Charts 10a and 10b, the tools and techniques used to obtain facts about the data breach are not the same ones they perceive should be used.

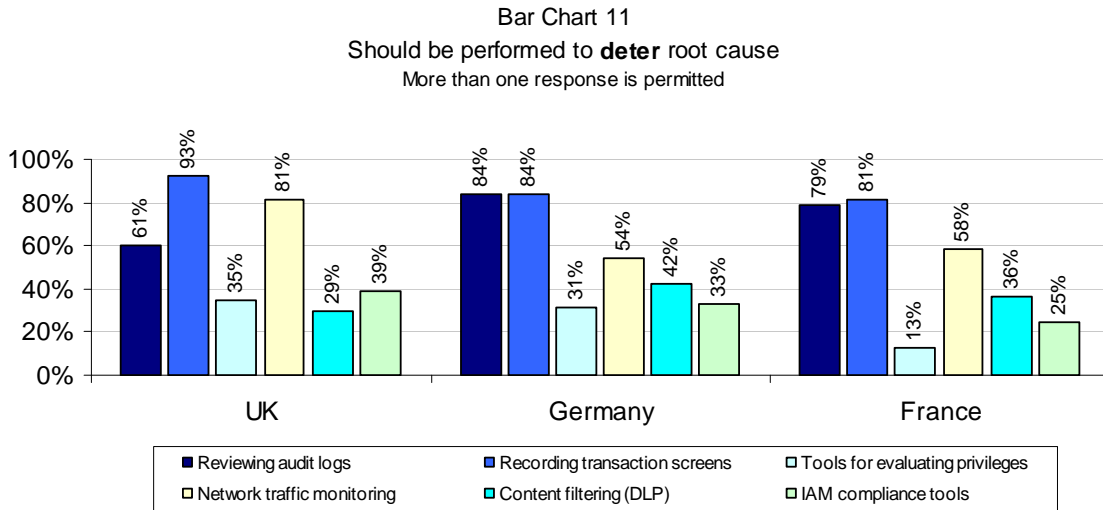


A solid majority (91% from the UK, 88% from Germany and 84% from France) believe that recording transaction screens for subsequent breach analysis is a technique that could serve as a deterrent to potential future data breach incidents. In sharp contrast, only 3% from the UK, 15% from Germany and 2% from France state that their organizations used record transaction screens to obtain facts about the data breach.

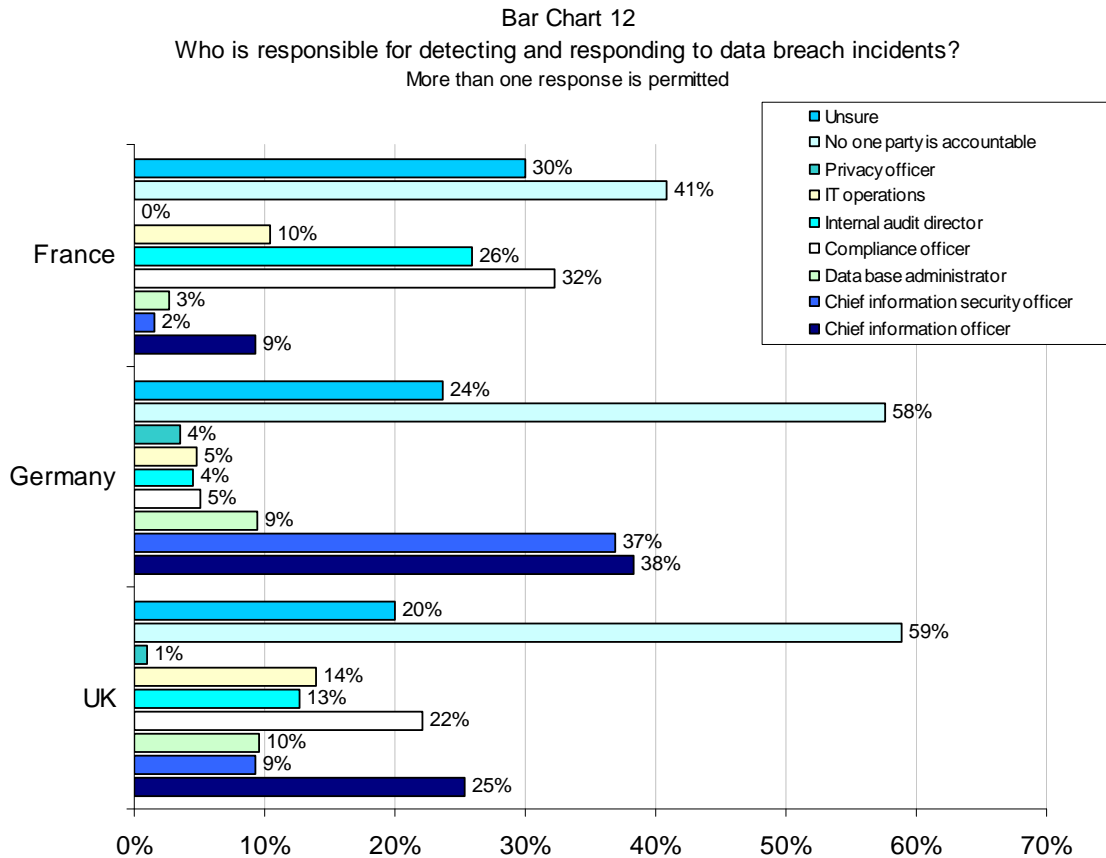


The second most popular technique that IT practitioners perceive should be in used in the UK and Germany is reviewing audit logs. In France it is the most popular technique. Furthermore, a

significant majority of respondents said that recording appropriate transaction screens for breach analysis and forensic evaluation would serve as a deterrent to potential future data breach incidents (see Bar Chart 11).



No one party is responsible for detecting and responding to a data breach.



As shown in Bar Chart 12, the largest number of respondents reports no one in their organization is accountable for data breach management (59% in the UK, 58% in Germany and 41% in

France). There is also uncertainty about who is responsible (20% in the UK, 24% in Germany and 30% in France). This obvious lack of accountability can have a negative affect not only on detecting data breaches but preventing them as well.

A lack of leadership in data breach management could contribute to the misallocation of resources and as a result not having the appropriate tools to detect and investigate data breaches. As shown above, IT practitioners believe they would use different tools and techniques to better understand the cause of the data breach. Better understanding of the root cause would lead to better approaches to deterring and preventing data breaches in the future.

Recommendations

The findings of this study indicate that data breaches continue to be a major problem for organizations. Unfortunately, as hard as it seems to prevent records from being lost or stolen they are often hard to detect.

The findings from this study indicate a serious governance issue—with no one function accountable or responsible for the management of a data breach detection, investigation and response program. In turn, without being able to understand the root cause of a data breach how can organizations prevent future incidents from occurring? Based on the results of the study, we recommend the following actions:

- Establish a data breach management governance framework. Accountability is required to detect data breaches and prevent future incidents.
- Establish criteria including scope, jurisdiction, type of data, source of breach (criminal vs. negligent insider) to determine which incidents require notification and how quickly notification should occur.
- Include plans to determine the scope of the breach. Limiting notification to the affected individuals not only saves on notification costs, but it also preserves your reputation.
- Plan and execute different scenarios to determine whether you have the appropriate forensic tools to quickly investigate a breach and determine its source. The results of your investigation should include an analysis of the security and archiving of forensic information to ensure a proper chain of evidence is met. Repeating this analysis on a recurring basis should ensure that you have appropriate evidence if needed.
- Prevent future data breaches by understanding the root causes of current data breaches. Consider options that will help deter breaches. Bar chart 10 identifies what respondents felt would be most useful in investigating and deterring breaches. Ninety percent of respondents indicated that recording authorized user activity and their access to sensitive data would be an effective deterrent. Notifying users of this monitoring may be required but will also increase the deterrence factor.
- Review your data access security to include portable devices, i.e. thumb drives, CDs, etc. Off-network devices and networks are considered most at risk and are most vulnerable to what are considered the causes of breaches—negligent insiders and outsourced data.
- Implement tools and techniques to detect and deter a breach. IT practitioners report that information about the data breach victim are the facts most often missing when investigating a data breach, which makes it difficult to respond in a timely manner as required by data breach notification laws.

In addition, the right tools and techniques to record application activity benefits forensic investigations. In January 2008, Societe Generale reported a €4.9 billion trading loss caused by an insider who carried out fraudulent transactions linked to rising stock markets. These

transactions, it is reported, were hidden through extremely sophisticated and varied techniques. The trades first came to management’s attention when a compliance officer found a trade that exceeded the bank’s limits. Recording the user’s application activity could have helped Societe Generale detect and potentially deter a breach such as this.

Caveats to this survey

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 information security practitioners. 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 a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- 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.

Samples for the UK, Germany and France

Sampling frames of adult-aged individuals who reside within the United Kingdom, Germany or France were used to recruit participants to three separate web surveys.¹ These sampling frames were selected from national mailing lists of IT professionals. Table 1 summarizes the results of our sampling plan for three countries.

Table 1 Sampling data for UK, Germany and France	UK	Germany	France
Overall sampling frame	13,932	14,908	14,031
Total returns	819	1008	759
Reliability rejects	34	45	23
Total sample	785	963	736
Response rate	5.63%	6.46%	5.25%

The net response rate is 5.63% for the UK, 6.46% for Germany and 5.25% for France. The margin of error on all adjective scale and Yes/No/Unsure responses is ≤ 3.25%. Table 2 provides the self-reported organizational level of respondents in the UK, Germany and France. As can be seen, the majority of respondents are at the staff/technician or manger/supervisor levels, respectively.

¹ Respondents were given nominal compensation to complete all survey questions.

Table 2: Organizational levels	UK	Germany	France
Vice President	1%	1%	0%
Director	13%	15%	18%
Manager/supervisor	29%	38%	39%
Staff/technician	46%	42%	41%
Other	11%	4%	2%
Total	100%	100%	100%

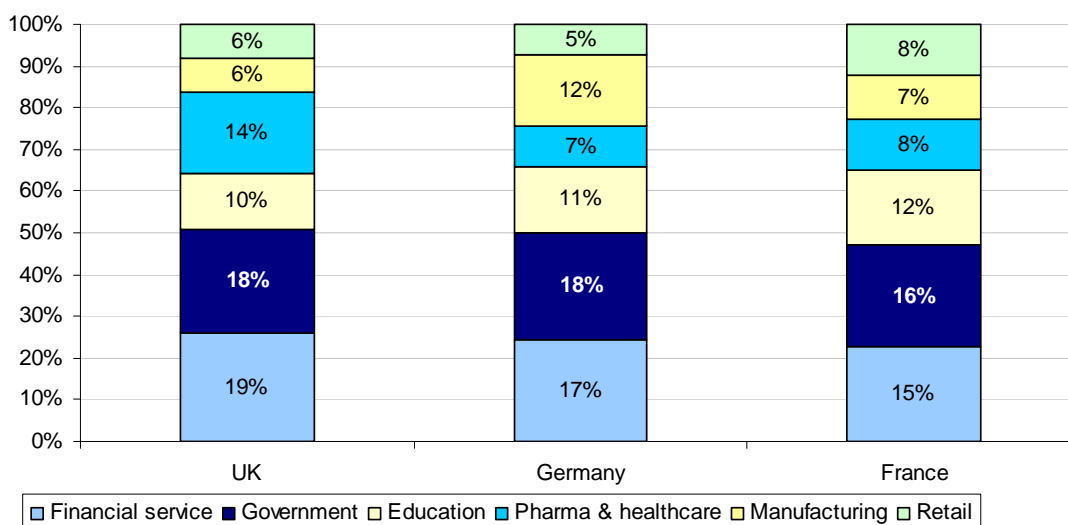
On average, respondents have more than eight (8) years of experience in the information management or security fields, and three years of experience in their current position. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the corporate IT fields for these European countries.

The majority of respondents' companies work for organizations that are closely held (not publicly traded or governmental entities). Table 3 provides the approximate headcounts of these organizations. As can be seen, most respondents are employed by larger-sized organizations as defined by organizational headcount of 5,000 or more full time equivalent employees.

Table 3. Corporate headcount	UK	Germany	France
Less than 500 people	2%	13%	0%
500 to 1,000 people	6%	5%	0%
1,001 to 5,000 people	21%	23%	18%
5,001 to 25,000 people	42%	28%	39%
25,001 to 75,000 people	23%	26%	41%
More than 75,000 people	6%	5%	2%
Total	100%	100%	100%

Bar Chart 13 reports the average distribution of respondents according to six major industry classifications.

Bar Chart 13
Largest industry categories for UK, Germany and France panels



As shown above, a large number of respondents are employed by financial service companies including insurance, banking, credit cards, brokerage and investment management. Another large

segment represents IT employees in central or local government. Other large industry groups included national samples include pharma/healthcare, manufacturing and retail.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, phone call or e-mail:

Ponemon Institute LLC
Attn: Research Department
2308 US 31North
Traverse City, Michigan 49686
1.800.887.3118
research@ponemon.org

Ponemon Institute LLC

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 organizations.

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.

Appendix: Survey Questions in Percentage Frequency Format

The following tables report key survey sampling statistics for research conducted in the United Kingdom (UK), Germany and France.

Description of the US, UK, DE & FR samples	UK	Germany	France
Overall sampling frame	13932	14908	14031
Invitations sent	8562	9905	7813
Bounce back	1113	884	673
Total returns	819	1008	759
Reliability rejects	34	45	23
Total sample	785	963	736
Response rate	5.6%	6.5%	5.2%

Part I: Were you involved in a data breach event?

Q1a. Has your organization experienced one or more data breaches involving the loss or theft of information about people or households (personal information)?	UK	Germany	France
Yes	55%	39%	62%
No (stop)	45%	61%	38%
Total	100%	100%	100%

Remaining sample	428	373	460
-------------------------	------------	------------	------------

Q1b. How were you involved? Please check all that apply.	UK	Germany	France
Defining response plan	6%	4%	4%
Establishing incident response team	14%	9%	5%
Training and educating staff and employees	27%	15%	39%
Detecting, verifying, investigating facts, and categorizing incidents	35%	80%	27%
Determining appropriate response (including internal escalation)	25%	7%	5%
Notifying parties /communicating with consumers, employees, shareholders and others	5%	2%	1%
Preparing reports to management	5%	4%	10%
Conducting root-cause analysis	36%	50%	10%
Remediation activities	32%	23%	15%
Interacting with regulatory/legal authorities/outside lawyers	1%	2%	4%
Other (please specify)	3%	7%	7%
None of the above (stop)	2%	2%	2%
Total	190%	205%	128%

Remaining sample	420	367	450
-------------------------	------------	------------	------------

Q2. How many data breach incidents involving the loss or theft of personal information occurred within your organization in the past 24 months?	UK	Germany	France
Only once	36%	49%	51%
About two to three incidents	21%	24%	9%
About four to five incidents	22%	7%	10%
More than five incidents	5%	13%	10%
Unsure	15%	8%	20%
Total	100%	100%	100%

Q3. How confident are you that all data breaches involving the loss or theft of personal information will be detected within your organization?	UK	Germany	France
Very confident	20%	25%	17%
Confident	34%	29%	34%
Somewhat confident	17%	34%	20%
Not confident	14%	5%	24%
Unsure	14%	8%	5%
Total	100%	100%	100%

Q4. In what IT environments did your organization's data breach incident occur? Please check all that apply.	UK	Germany	France
Mainframes	38%	34%	38%
Networks	60%	45%	91%
Backups	12%	12%	24%
Off-network devices	51%	42%	38%
Paper files	54%	14%	17%
Other	6%	7%	5%
Total	221%	154%	214%

Q5. What has been the most likely cause(s) of data breaches within your organization? Please check all that apply.	UK	Germany	France
External attack (hackers)	3%	9%	6%
Social engineering or pre-texting	6%	7%	8%
Negligent insiders	63%	46%	52%
Malicious insiders	37%	24%	38%
outsourced data	25%	11%	39%
Other	4%	7%	4%
Total	139%	104%	147%

Part II: Please respond based on the most recent data breach caused by an insider (including outsourcers) involving the loss or theft of personal information your organization experienced.

Q6a. Did this data breach incident require notification of individuals whose personal information was lost or stolen?	UK	Germany	France
Yes	19%	9%	5%
No	81%	91%	95%
Total	100%	100%	100%

Q6b. If yes , after discovering the incident, how much time did it take for your organization to respond to data breach victims who required notification?	UK	Germany	France
Immediately	20%	34%	72%
Within a few days	28%	58%	28%
Within a few weeks	41%	3%	0%
Within one month	3%	0%	0%
More than one month	8%	0%	0%
Total	100%	95%	100%

Q7. In your opinion, how important is it for your organization to respond quickly to data breach victims who require notification?	UK	Germany	France
Very important	36%	52%	38%
Important	33%	38%	45%
Somewhat important	19%	10%	14%
Not important	10%	0%	2%
Irrelevant	3%	0%	0%
Total	100%	100%	100%

Q8a. In your opinion, were you able to determine all relevant facts – that is, the “who, what, where, when and how” – in order to pinpoint the root cause of the incident as well as who needs to be notified?	UK	Germany	France
Yes	85%	70%	65%
No (Go to 8d)	15%	30%	35%
Total	100%	100%	100%

Q8b. If yes , how confident do you feel that you and your organization obtained <u>all the facts</u> associated with this data breach incident?	UK	Germany	France
Very confident	5%	5%	12%
Confident	39%	27%	20%
Somewhat confident	32%	32%	36%
Not confident	17%	26%	25%
Unsure	8%	10%	8%
Total	100%	100%	100%

Q8c. If yes , what facts did you gather to detect and appropriately respond to the data breach event?	UK	Germany	France
Nature of the incident (i.e., negligence or criminal intent)	51%	52%	24%
Source of the incident (i.e., privileged users, general employees, contractors and/or IT glitches that caused the event)	52%	70%	35%
Types of files or data-bearing electronic device lost or stolen	73%	72%	65%
Types of information (i.e., customer, employee, consumer)	70%	78%	68%
People whose information was lost or stolen (i.e., victim)	74%	39%	26%
Impact or harm resulting from the data breach	15%	19%	14%
The recipient(s) of the information	30%	41%	9%
Date and time of the actual incident	47%	63%	30%
Regulatory and legal requirements	15%	30%	27%
Other (please specify)	8%	5%	3%
Total	435%	469%	300%

Q8d. If no , what facts were missing to detect and appropriately respond to the data breach event?	UK	Germany	France
Nature of the incident (i.e., negligence or criminal intent)	55%	47%	48%
Source of the incident (i.e., privileged users, general employees, contractors and/or IT glitches that caused the event)	81%	63%	70%
Types of files or data-bearing electronic device lost or stolen	64%	33%	49%
Types of information (i.e., customer, employee, consumer)	68%	66%	64%
People whose information was lost or stolen (i.e., victim)	74%	78%	81%
Impact or harm resulting from the data breach	60%	76%	89%
The recipient(s) of the information	52%	52%	58%
Date and time of the actual incident	39%	52%	88%
Regulatory and legal requirements	20%	5%	8%
Other	2%	3%	8%
Total	514%	476%	563%

Q9. For each fact listed below, please check how important it is for understanding the cause of the breach? 1=very important, 2=important, 3=somewhat important, 4=not important, 5=irrelevant.	1	2	3	4	5	UK Total
Nature of the incident (i.e., negligence or criminal intent)	24%	27%	34%	14%	2%	100%
Source of the incident (i.e., employees, contractors and/or IT glitches that caused the event)	26%	16%	36%	16%	7%	100%
Files or data-bearing electronic devices lost or stolen	22%	32%	32%	12%	2%	100%
Information lost or stolen (i.e., customer, employee, consumer, business confidential, intellectual property)	31%	29%	31%	4%	6%	100%
People whose personal information was lost or stolen (i.e., victims who may require notification)	19%	29%	28%	19%	5%	100%
Impact or harm resulting from the data breach	17%	30%	39%	13%	1%	100%
Recipients of the information	32%	42%	22%	5%	0%	100%
Date and time of the actual incident	23%	33%	13%	23%	6%	100%
Regulatory and legal requirements	2%	12%	62%	12%	13%	100%

Q9. For each fact listed below, please check how important it is for understanding the cause of the breach? 1=very important, 2=important, 3=somewhat important, 4=not important, 5=irrelevant.	1	2	3	4	5	Germany Total
Nature of the incident (i.e., negligence or criminal intent)	12%	32%	40%	15%	1%	100%
Source of the incident (i.e., employees, contractors and/or IT glitches that caused the event)	17%	33%	32%	12%	7%	100%
Files or data-bearing electronic devices lost or stolen	6%	20%	37%	28%	10%	100%
Information lost or stolen (i.e., customer, employee, consumer, business confidential, intellectual property)	21%	20%	30%	22%	7%	100%
People whose personal information was lost or stolen (i.e., victims who may require notification)	10%	13%	41%	28%	7%	100%
Impact or harm resulting from the data breach	3%	11%	40%	43%	3%	100%
Recipients of the information	21%	30%	29%	16%	4%	100%
Date and time of the actual incident	2%	14%	57%	8%	19%	100%
Regulatory and legal requirements	10%	3%	70%	16%	1%	100%

Q9. For each fact listed below, please check how important it is for understanding the cause of the breach? 1=very important, 2=important, 3=somewhat important, 4=not important, 5=irrelevant.	1	2	3	4	5	France Total
Nature of the incident (i.e., negligence or criminal intent)	20%	25%	30%	23%	2%	100%
Source of the incident (i.e., employees, contractors and/or IT glitches that caused the event)	24%	29%	22%	18%	6%	100%
Files or data-bearing electronic devices lost or stolen	18%	30%	31%	17%	4%	100%
Information lost or stolen (i.e., customer, employee, consumer, business confidential, intellectual property)	19%	28%	36%	16%	1%	100%
People whose personal information was lost or stolen (i.e., victims who may require notification)	22%	33%	27%	17%	2%	100%
Impact or harm resulting from the data breach	4%	21%	54%	18%	4%	100%
Recipients of the information	11%	15%	52%	16%	6%	100%
Date and time of the actual incident	5%	28%	47%	3%	18%	100%
Regulatory and legal requirements	16%	22%	44%	14%	5%	100%

Q10. What tools or techniques did your organization use to obtain facts about the data breach incident? Please check all that applied to your investigation:	UK	Germany	France
Tools that reviewed system audit logs.	43%	84%	37%
Used content filtering to match key terms or phrases in documents	15%	33%	29%
Used sniffing to identify errors, irregularities or inconsistencies in networks and websites	9%	35%	3%
Evaluated end-user permissions such as opt-in or opt-out	32%	43%	21%
Recorded appropriate transaction screens for breach analysis and forensic evaluation	3%	15%	2%
Determined compliance of identity and access management procedures	17%	33%	18%
Evaluated information for accuracy and quality	33%	28%	56%
Checked for alterations in backup and recovery procedures	6%	42%	53%
Reviewed software patch activity	44%	76%	39%
Recorded network traffic for surveillance and forensic evaluation	9%	52%	60%
None of the above tools were available	28%	4%	7%
Other	8%	23%	7%
Total	249%	468%	332%

Q11. What tools or techniques do you believe your organization should have to obtain facts about the data breach incident? Please check all that apply:	UK	Germany	France
Tools to facilitate the review of system audit logs	66%	80%	84%
Detection or prevention of intrusions to enterprise systems and networks	44%	35%	26%
Content filtering to match key terms or phrases in documents	34%	46%	31%
Sniffing to identify errors, irregularities or inconsistencies in networks and websites	19%	37%	24%
Evaluation of end-user permissions such as opt-in or opt-out	56%	50%	57%
Record appropriate transaction screens for breach analysis and forensic evaluation	91%	88%	79%
Determine compliance of identity and access management procedures	38%	31%	36%
Evaluate information accuracy and quality	10%	18%	9%
Check for alterations in backup and recovery procedures	23%	17%	20%
Review of software patch activity	8%	12%	14%
Record network traffic for surveillance and forensic evaluation	40%	56%	55%
Other	19%	15%	15%
Total	448%	485%	450%

Q12. What tools or techniques do you believe could serve as a deterrent to potential future data breach incidents? Please check all that apply:	UK	Germany	France
Tools to facilitate the review of system audit logs	61%	84%	79%
Detection or prevention of intrusions to enterprise systems and networks	39%	33%	25%
Content filtering to match key terms or phrases in documents	29%	42%	36%
Sniffing to identify errors, irregularities or inconsistencies in networks and websites	53%	49%	72%
Evaluation of end-user permissions such as opt-in or opt-out	35%	31%	13%
Record appropriate transaction screens for breach analysis and forensic evaluation	93%	84%	81%
Determine compliance of identity and access management procedures	37%	32%	43%
Evaluate information accuracy and quality	13%	17%	9%
Check for alterations in backup and recovery procedures	29%	24%	16%
Review software patch activity	10%	7%	5%
Record network traffic for surveillance and forensic evaluation	81%	54%	58%
Announce and record transaction activity	38%	46%	11%
Securely archive recorded transaction activity	54%	68%	25%
Other	1%	0%	0%
Total	573%	570%	473%

For each question listed below, please check 1=very important, 2=important, 3=somewhat important, 4=not important, 5=irrelevant.	1	2	3	4	5	UK Total
Q13. Are automated tools important to your overall audit and compliance mission?	35%	24%	38%	4%	0%	100%
Q14. How important are tools that help you and your organization perform forensic activities when determining the cause and effect of a data breach?	8%	31%	52%	5%	3%	100%
Q15. How important are tools that help you and your organization deter employee or contractor negligent or malicious behaviors that may cause future data breaches?	51%	26%	21%	1%	0%	100%

For each question listed below, please check 1=very important, 2=important, 3=somewhat important, 4=not important, 5=irrelevant.	1	2	3	4	5	Germany Total
Q13. Are automated tools important to your overall audit and compliance mission?	35%	27%	16%	4%	18%	100%
Q14. How important are tools that help you and your organization perform forensic activities when determining the cause and effect of a data breach?	28%	29%	42%	1%	0%	100%
Q15. How important are tools that help you and your organization deter employee or contractor negligent or malicious behaviors that may cause future data breaches?	45%	23%	23%	6%	2%	100%

For each question listed below, please check 1=very important, 2=important, 3=somewhat important, 4=not important, 5=irrelevant.	1	2	3	4	5	France Total
Q13. Are automated tools important to your overall audit and compliance mission?	37%	19%	30%	7%	7%	100%
Q14. How important are tools that help you and your organization perform forensic activities when determining the cause and effect of a data breach?	3%	28%	47%	6%	16%	100%
Q15. How important are tools that help you and your organization deter employee or contractor negligent or malicious behaviors that may cause future data breaches?	48%	28%	23%	1%	0%	100%

Q16. Please check all the regulations listed below that are most influential to your organization's IT security policies and programs:	UK	Germany	France
Breach notification statutes	14%	NA	NA
Sarbanes-Oxley	32%	8%	7%
Payment Card Industry (PCI) requirements	25%	7%	4%
Gramm-Leach-Bliley Act	NA	NA	NA
National privacy & data protection laws	12%	47%	54%
FTC Safeguards Rule	NA	NA	NA
European Union Privacy Directive	26%	41%	45%
Health Insurance Portability & Accountability Act	NA	NA	NA
Financial Service Authority (FSA)	19%	NA	NA
Other	5%	17%	15%
Total	132%	120%	125%

Q17. Who is responsible within your organization for detecting or responding to a data breach incident? Please check all that apply:	UK	Germany	France
Chief information officer	25%	38%	9%
Chief information security officer	9%	37%	2%
Data base administrator	10%	9%	3%
Compliance officer	22%	5%	32%
Internal audit director	13%	4%	26%
IT operations	14%	5%	10%
Privacy officer	1%	4%	0%
No one party is accountable	59%	58%	41%
Unsure	20%	24%	30%
Other	3%	1%	3%
Total	378%	436%	453%