



Privacy & Data Protection Practices

Benchmark Study of the Financial Services Industry

Sponsored by Compuware

Conducted by Ponemon Institute LLC

January 31, 2010

Privacy & Data Protection Practices

A Benchmark Study of the Financial Services Industry

Presented by Ponemon Institute, January 31, 2010

I. Executive Summary

Privacy & Data Protection Practices: a Benchmark Study of the Financial Services Industry was conducted by Ponemon Institute and sponsored by Compuware to learn how effectively companies are managing their privacy and data protection risks. We believe the results of this study will help companies determine how comprehensive their privacy and data protection program is compared to other financial services organizations. The study also provides guidance on how to address any areas where organizations may not be in compliance with regulations or vulnerable to a data breach.

The findings of this study reveal that despite the numerous privacy regulations ranging from Gramm-Leach-Bliley to the recent Red Flags Rule, the vast majority of participating financial institutions have significant gaps in their privacy and data protection programs. We believe the most significant gaps are in the areas of addressing the insider threat, the outsourcing of sensitive data to third parties and issues related to customer trust.

In this benchmark study, we interviewed the chief security officer, the chief information security officer, the chief privacy officer or another individual who has overall responsibility for privacy and data protection. A total of 80¹ multinational organizations participated in this research study. The types of financial organizations in this study are: banking, investment, brokerage, insurance, credit card, and mortgage. We used a standardized benchmark instrument that covered the following topics:

- Policies and procedures
- Training, awareness and communications
- Program management activities
- Data security features, including data testing environments both internal and outsourced
- Third-party data vendor agreements
- Compliance, monitoring and audit
- Redress and enforcement

In the case of compliance, we considered eight (8) major regulations affecting the financial services industry. These are listed in Table 1 below. While not an exhaustive list of regulatory requirements, our goal was to determine if organizations in our study are taking appropriate steps to comply with privacy and data protection requirements or if there are any gaps in an organization's compliance with these regulations. For example, we asked questions about practices involving the sharing of personal information with third parties and providing opt-out over secondary use of personal information.

The percentages shown in Table 1 indicate the frequency of companies that appear to achieve substantial compliance (i.e., shown in the Minimal Compliance Gaps column) or appear to be inadequate in meeting these requirements (i.e., shown in the Significant Compliance Gaps column). According to Table 1, there are no significant compliance gaps with the Children's Online Privacy Protection Act. However, this is not the case with the Red Flags Rule where 35 percent of organizations have significant compliance gaps.² Later in this paper, we describe other gaps participating organizations have with regulations (see page 8).

¹ A total of 80 companies, of which 63 were separate organizations, participated in the study.

² Please note that the columns in Table 1 do not sum to 100 percent. The difference in percentage represents organizations' compliance programs that fall between minimal and significant compliance gaps.

Table 1 Financial Service Privacy Regulations	Minimal Compliance Gaps	Significant Compliance Gaps
Children's' Online Privacy Protection Act	71%	0%
Gramm-Leach-Bliley Act	59%	10%
Basel II Accord	55%	19%
Fair Credit Reporting Act	54%	13%
Fair & Accurate Credit Transactions Act	52%	20%
Safeguards Rule (FTC)	46%	29%
Red Flags Rule (FTC)	45%	35%
Federal Financial Institution's Examine Council (FFIEC) Guidelines	43%	25%

II. Key Findings

Based on Ponemon Institute research, the six areas of greatest vulnerability to privacy and data protection threats in organizations are discussed below. These are: risk of a data breach, diminishment of customer loyalty and trust, malicious or negligent insiders, the risk of outsourcing sensitive and confidential data to third parties, compliance with regulations, especially the Red Flags Rule and ineffective privacy and information security governance. The benchmark results show how well or poorly financial organizations in our study are responding to these risks.

Risk of a data breach

Most of the individuals we interviewed in this study believe that senior management (C-level executives) are out-of-touch with serious security issues such as the growing threat of cyber criminals and increasing incidents of data theft. This lack of awareness can hinder the ability to secure adequate funding and support. Therefore, how successful are companies at responding to information security threats?

We determined the top security practices in use are: physical security safeguards that prevent access to storage devices containing consumer or customer information, technologies or other means to identify or prevent unauthorized or illegal movement or transfer of data or documents, steps to secure Social Security numbers. However, very few have an inventory of all applications and technologies that use customer or consumer information.

It is very positive to see that the majority of organizations (76 percent) have a data protection security or plan. However, less than half (47 percent) review new software applications and databases for privacy considerations and compliance to law before placed in operation.

We found it concerning that only 12 percent of companies in our study **do not use** Social Security numbers of their customers for primary identification purposes. However, 88 percent of organizations say they take appropriate steps to secure the use of Social Security numbers. They are doing this through special policies for handling this data or visually blocking Social Security numbers from user/operator views.

Over 83 percent of companies use, real (live) customer or employee information in development and testing, and 51 percent of these companies admit they **do not take** appropriate steps to protect real data used in development and testing such as anonymization of data, masking, subsetting or other methods.

The technologies most used by organizations in our study to prevent data loss and theft include the following:

- Technologies used to identify unauthorized or illegal movement or transfer of data or documents (87 percent).
- SSL on all web forms containing sensitive personal information (92 percent).
- Authentication of all visitors to all websites that contain sensitive or confidential information (85 percent).
- Authentication to determine who has access to personal information (75 percent).
- Use of encryption in the exchange of customer information (88 percent).
- Use of encryption in securing information in storage (85 percent).
- Multilayered firewall protection over consumer or customer data (100 percent).
- Dual authentication to limit or control access to sensitive or confidential information (79 percent).

Eighty-one percent have their data storage devices in physically secure areas and 88 percent have physical security safeguards that prevent access to storage devices containing consumer or customer information.

We believe the following practices are not used as widely as they should be. Thus creating gaps in organizations' approaches to reducing the risk of data loss or theft (a.k.a. data breach):

- Identity compliance procedures to ensure that user access rights are accurate, complete and appropriately specified to fulfill a given set of business functions in use by 56 percent of organizations.
- The use of data loss prevention solutions to curtail the leakage of consumer or customer information in use by 41 percent of organizations.
- Intrusion detection systems in use by 47 percent of organizations.
- Protection of real data used in development and testing in use by 49 percent of organizations.

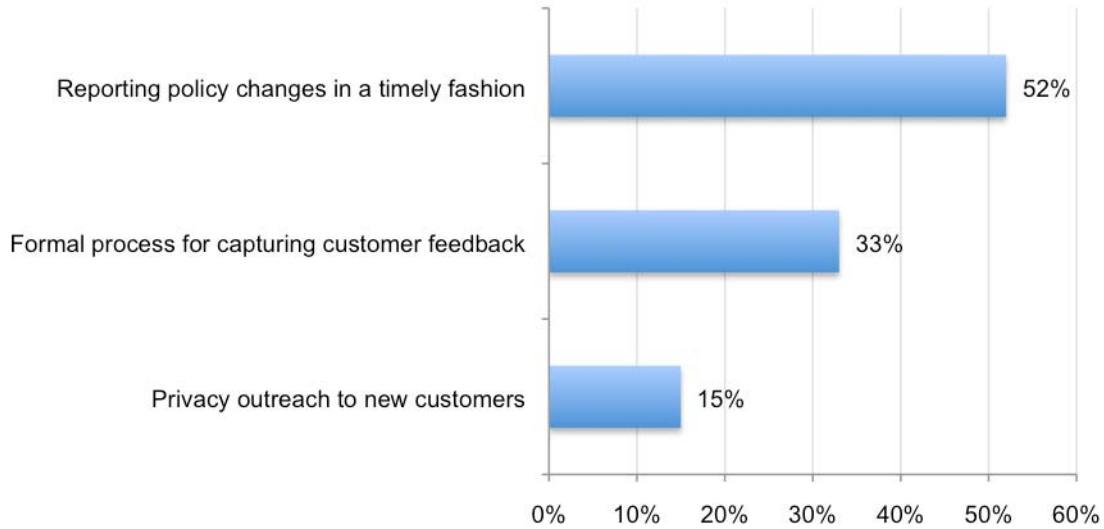
Diminishment of customer loyalty and trust

Are financial organizations taking appropriate steps to achieve and maintain a trusted relationship with their customers? Are they respecting the privacy preferences of their customers and providing enough opportunities to communicate these preferences? While it is critical to protect data from a breach, it is also important to respect consumers' preferences about how their data is shared with third parties.

We found many organizations are cognizant of the need to communicate how they are protecting sensitive information and whether this information is being shared with third parties. However, many organizations are not taking additional steps to make sure consumers' preferences are being honored. This is especially the case with practices governing access and redress.

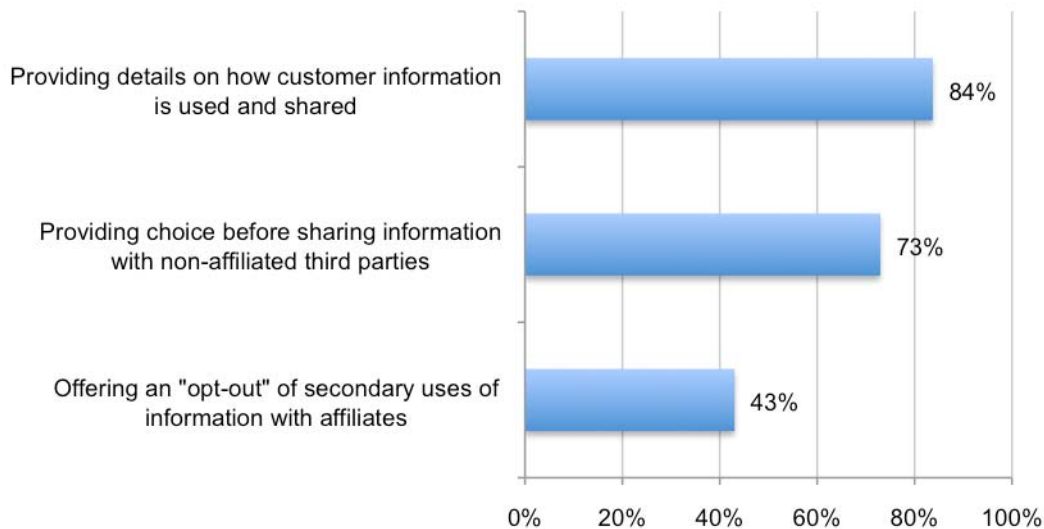
Bar Chart 1 shows that more than half (52 percent) of organizations take communications with their customers seriously and have a process for making sure any significant changes in the company's privacy policy are reported to them in a timely fashion. However, only 33 percent have a formal process for capturing feedback from customers or consumers who have additional questions about the policy or notice they receive from the organization. Fifteen percent have a privacy awareness or outreach effort for new customers.

Bar Chart 1
Communication practices with customers



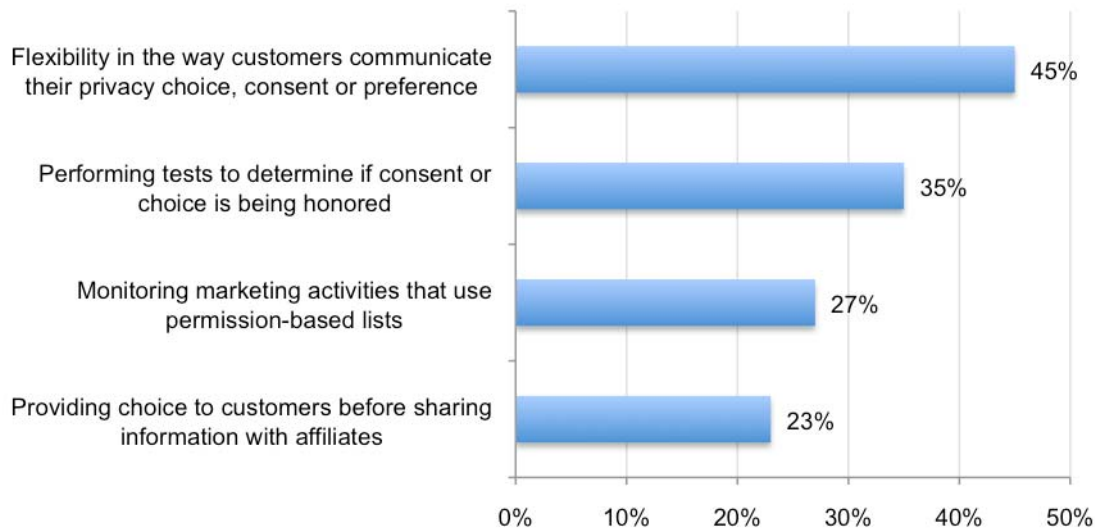
An area of concern to consumers is how their customer information will be used and shared. As shown in Bar Chart 2, most organizations in the study are responsive to these concerns. Eighty-four percent provide adequate details on how customer information will be used and shared and 73 percent provide choice to customers before sharing information with non-affiliated third parties. An area that could be improved is the sharing of information with affiliates. Less than half (43 percent) are offering an opt-out of secondary uses of their information with affiliates.

Bar Chart 2
Information use and sharing practices



As shown in Bar Chart 3, less than half (45 percent) offer flexibility in the way their customers communicate their privacy choice, consent or preference. Thirty-five percent perform tests to determine if consent or choice is being honored and 27 percent monitor marketing activities that use permission-based lists. Only 23 percent provide choice to customers before sharing information with affiliates.

Bar Chart 3
Customer preference management practices



In the case of redress and enforcement, 65 percent have a redress process clearly described in the privacy notice or policy and the same percentage have a formal process for reporting privacy or security breaches to data subjects involved in the breach. However, not many organizations in our study have adopted practices important to addressing the privacy concerns of customers and consumers. Following are privacy and data protection practices critical to building trust and loyalty with consumers. As shown below, the percentage of financial service organizations adopting these practices is relatively low:

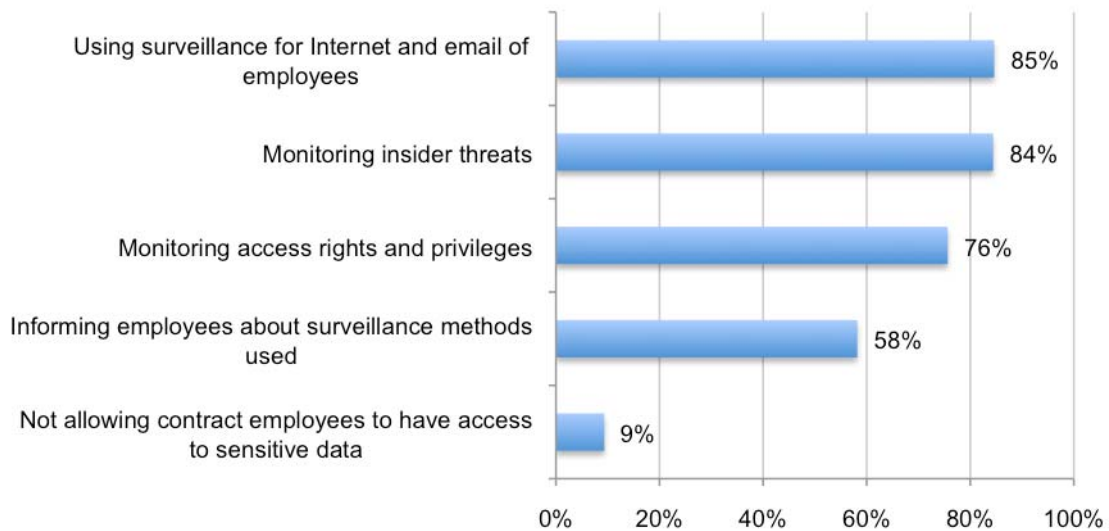
- Consumer access to view and correct their personal information (25 percent).
- Customer and consumer access to a redress procedure for resolving privacy concerns (24 percent).
- Mediation or arbitration on privacy matters (26 percent).
- Access to the privacy leader (11 percent).
- A helpline for customers and consumers to ask questions or report a problem about privacy (32 percent).
- The use of mystery shopping techniques to test the privacy “readiness” of customer services (11 percent).
- A standardized process for responding to helpline calls (40 percent).
- Education of call center employees on how to respond and escalate privacy complaints (25 percent).
- A specific timeline for investigating alleged privacy complaints (15 percent).
- A redress process that has specific reporting requirements to management (11 percent).

Malicious or negligent insiders

As established in many Ponemon Institute studies, IT and IT security practitioners consider malicious or negligent insiders to be one of the top reasons data breaches occur. How well are organizations in this study addressing the insider threat? It seems that most organizations are monitoring insider threats and using some form of surveillance to reduce this risk. They are also making sure employees and temporary employees have appropriate access rights. However, we believe many organizations in this study are putting data at risk by not having appropriate training for employees who handle customers’ sensitive and confidential information. Further, they do not test for the effectiveness of training.

According to the results of the study as reported in Bar Chart 4 below, 84 percent of companies monitor insider threats such as negligence or malicious employees and 85 percent use surveillance methods to monitor the Internet and email of employees. Fifty-eight percent of companies inform employees about the use of surveillance. Only 9 percent of companies do not allow contract employees to have access to sensitive data.

Bar Chart 4
Practices to manage insider threats



To ensure sensitive data is not available to unauthorized individuals, 76 percent of companies monitor access rights and privileges such as revoking access rights when employees or temporary employees are terminated. Only 9 percent do not allow contract employees to have access to sensitive data.

Bar Chart 5
Privacy training practices

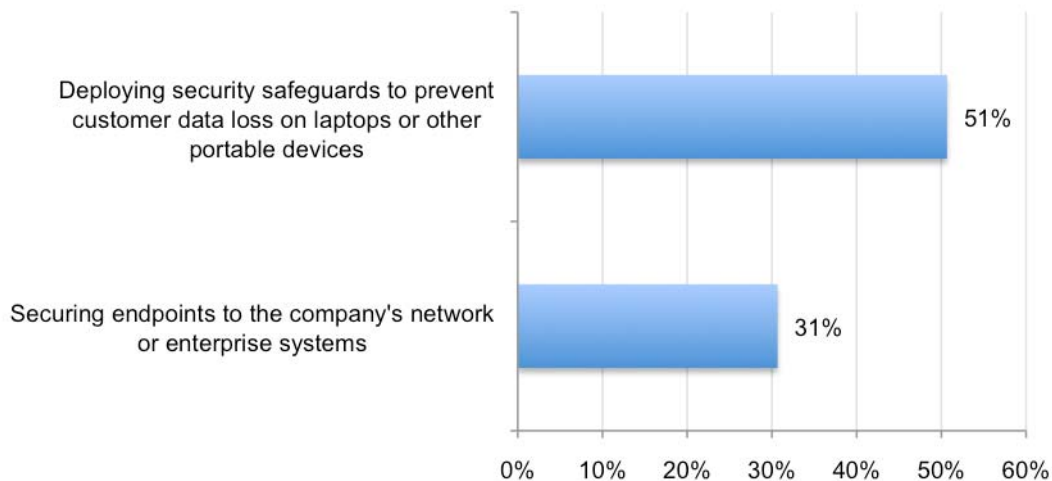


While not shown in Bar Chart 5, 57 percent of organizations have a process for communicating the privacy policy to all employees who interact with customer data. Interact means use, create, change, store, manage and destroy records about people and households. However, only 27 percent of organizations have privacy training programs that are assessed for effectiveness (Bar Chart 5). Only 31 percent have training available on demand (such as CBT or video) and only 16 percent communicate the results of privacy training to the company’s privacy leader or other senior executive.

While more than half (56 percent) perform background checks on all privileged users (such as system administrators) and contractors before they are granted access to consumer, customer or employee data, we believe the 44 percent of organizations not following this basic procedure are putting their organizations at great risk for a data breach.

Mobility of the workforce is another insider risk faced by organizations. As shown in Bar Chart 6, 51 percent use security safeguards, such as whole disk encryption to prevent consumer or customer data on laptop computers or other portable devices from being lost or stolen. Only 31 percent report they sufficiently secure the company’s network or enterprise system. This is critical when organizations have employees, contractors and temporary employees accessing the network from remote locations.

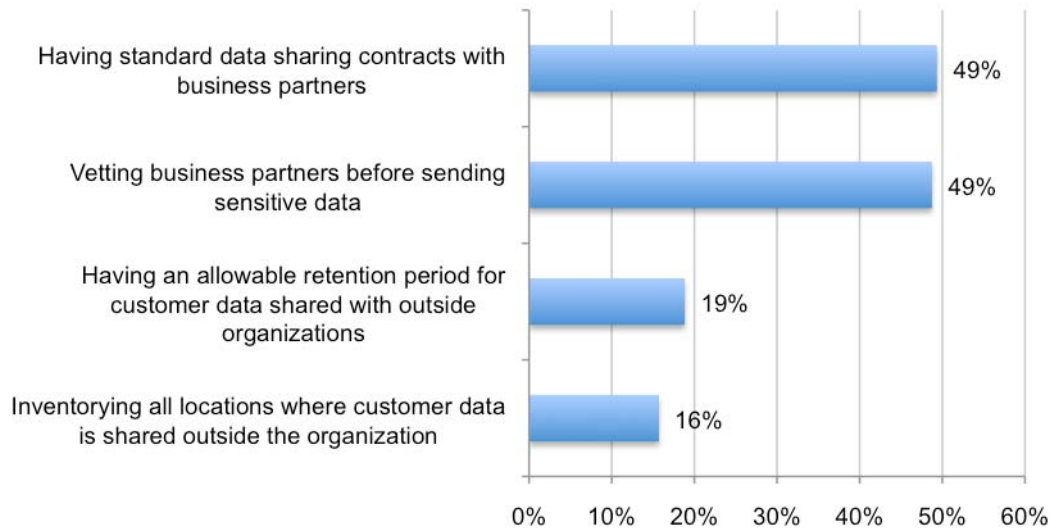
Bar Chart 6
Practices to manage threats posed by mobile workforce



The risk of outsourcing sensitive and confidential data to third parties.

Despite the risk of a data breach when outsourcing confidential and sensitive data to third parties, only 49 percent of organizations in our study perform reviews or vet business partners before sending data about customers, consumers, employees and others (see Bar Chart 7). Further only 49 percent have standard contracts with business partners containing language that ensures privacy protections over their data.

Bar Chart 7
Practices to manage third-party risks to customer information



Only 16 percent have an inventory of all locations where consumer or customer information is shared outside the organization (i.e. printing vendors, credit bureaus, affiliates) and 19 percent have signed agreements with outside entities on the allowable retention period for consumer or customer information.

Compliance with regulations, especially the Red Flags Rule

In the Executive Summary, we listed eight regulations affecting financial services organizations. Compliance ranged from no significant gaps (Children’s Online Privacy Protection Act) to significant compliance gaps (The Safeguards Rule and the new Red Flags Rule).

A majority of financial institutions in our study do not have adequate procedures in-place to comply with the new Red Flags Rule. These gaps in compliance include the lack of enterprise training, internal control procedures to monitor identity fraud and customer outreach procedures.

One positive finding of our study is that 86 percent of organizations say they implemented a Red Flags Rule program, and 65 percent say they have a Red Flags Rule program coordinated across the enterprise. However, as evidenced by their responses, we believe many organizations have the following gaps in compliance. Each percentage refers to organizations with the following procedures.

- Modify their know-your-customer polices to comply with the Red Flags Rule (33 percent).
- Have controls over paper documents containing protected customer information (43 percent).
- Have redress procedures for customers who are concerned about becoming an identity theft victim (30 percent).
- Review security systems and possibly modified them to ensure compliance with the Red Flags Rule (29 percent).
- Reduce the collection of unnecessary sensitive customer information in order to curtail identity theft (28 percent).
- Implement new or revised methods for tracking customer complaints that relate to concerns about identity theft (18 percent).

Ineffective privacy and information security governance puts sensitive and confidential information about customers, employees and others at risk.

Despite the complexity of privacy and data security laws and regulatory requirements, most financial institutions in our study do not have adequate staff or resources for accomplishing tactical objectives. The lack of resources appears to be a growing problem because of the current financial and marketplace conditions. Further, important governance practices such as privacy audits, records management procedures and practices to understand the root cause of a data breach are not in place in many of the organizations in our study.

A large number of institutions admit they do not have a high-level officer with overall privacy program responsibility. In many cases, the privacy program is not owned by any one individual or functional leader (but rather an ad hoc steering committee). Several financial services organizations admit that recent consolidation and acquisitions in the financial service marketplace have exacerbated privacy issues.

While 60 percent of organizations have a chief privacy officer, 50 percent report that they have insufficient resources to accomplish their goals and objectives. Other indications that ineffective privacy governance exists include the following (percentages indicate organizations with these practices in place).

- An independent privacy audit been conducted in the past two years (30 percent).
- Information security is integrated with privacy compliance (28 percent).
- Sufficient records management procedures are in place to ensure that documents containing consumer or customer information can be obtained easily, especially in the event of an e-discovery request (41 percent).
- Sufficient records management procedures are in place to ensure documents containing consumer or customer information are retained according to statutory requirements and not beyond these requirements (41 percent).
- Mock regulatory assessments are conducted to determine compliance with policy or law (13 percent).
- Sufficient procedures are in place to know or understand the root causes of most privacy violations or data breach incidents (41 percent).

III. Caveats on Benchmarks

There are inherent limitations to survey research that need to be carefully considered before drawing conclusions from findings. The following items are specific limitations that are germane to the present study.

- Non-statistical sample. The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative (non-statistical) sample of 80 financial service organizations, all located in the United States or Canada. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the nature and sampling process used.
- Non-response. The current findings are based on a small representative (non-statistical) sample of completed surveys. Benchmark survey instruments were distributed to companies in the financial services industry over a four-month period. Several benchmark survey instruments were sent directly to companies that have been involved in prior Ponemon Institute research activities.

- In total, 80 companies were selected for analysis in this report based on organizational size (i.e., those companies that employ more than 500 individuals). Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of benchmark performance criteria from those that completed the instrument.
- Sampling bias. We acknowledge that the quality of results may be biased in two important areas. First, all companies are North American-based financial service organizations. Hence, the results of our study can not be generalized to other parts of the world. Second, the companies represented here are mostly large, complex business organizations. Hence, it is impossible to generalize findings to a plethora of smaller-sized financial service organizations such as local or community banks.
- Company-specific information. The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.
- Unmeasured factors. To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.
- 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 accurate or truthful responses.

III. Benchmark Methods

The benchmark survey is designed to collect descriptive information from privacy and data protection practitioners in a timely and cost-efficient manner. The number of survey items is limited to key issues that cut across different programmatic activities. We believe that a survey focusing on operational process (rather than compliance issues) yields a higher response rate and better quality of results. We also use an actual paper or PDF instrument, rather than electronic (Web) survey, to provide greater assurances of confidentiality.

To keep the survey to a manageable size, we carefully limited items to only those business or operational factors that we consider crucial to the research objective. Hence, items focused on seven core areas of privacy management across the enterprise. It also included a special section on the Red Flags Rule, which at the time of this research has been postponed. Other descriptive items in the survey instrument explored key relationships between organizational variables and descriptive responses to benchmark items.

Ponemon Institute developed a revised survey instrument based on comments received by Compuware as well as several leaders in the privacy community. For purposes of consistency, most survey items from the first benchmark study were held constant.³ Additional items were included in the data security and compliance management categories to accommodate new developments in the privacy and data protection fields. The final instrument was assessed for clarity and function with the approval of the sponsor.

In total, the benchmark survey instrument contains 155 descriptive items. The survey all captured organizational demographic items for sample analysis and comparison. A fixed-format design is used for capturing responses to all benchmark items. The following are the fixed response categories to all benchmark items:

- Yes – denotes a positive response to one survey item.
- No – denotes a negative response to one survey item.
- Unsure – denotes sufficient information available to the individual responding to one survey item.
- Exception – which is additional contextual information to explain, Yes, No or Unsure responses to each given survey item. This data is optional only.
- Blank – This is a no comment response and is not counted in the analysis.

Analysis of benchmark responses focuses on the percent of positive (Yes) responses, defined as:

$$\text{Yes Response} = \text{Yes (Adjusted for Reverse Scored Items)} \div (\text{No} + \text{Unsure}).$$

The percent of Yes response variable is our surrogate for measuring good privacy practices.⁴ No, unsure or blank responses provide insufficient information to draw any conclusions about the efficacy of corporate privacy efforts.

A secondary variable reported in the analysis is the percent of completion. A 100% completion rate means that all participating companies responded to the item with either a yes, no or unsure response (i.e., no blanks). The average percent of completion to all 155 items is 89%, with the lowest completion rate at 50%.

To maintain complete confidentiality, the survey instrument does not capture company-specific information of any kind. Subject materials contain no tracking codes or other methods that could link responses to specific organizations. In some instances, subjects returned their survey in a standard business envelope. In these cases, we removed the instrument and destroyed the envelope. In other instances, individuals sent their completed survey through e-mail. Again, in these cases, the instrument was printed and the e-mail deleted.

³ Ponemon Institute conducted the first benchmark study on privacy and data protection practices in 2003.

⁴ Many benchmark survey responses indicated a Yes response, but only for a portion or part of the organization's privacy initiatives. For purposes of consistency, a partial Yes response was recorded as Yes rather than as Unsure or No.

When we entered the survey information, each instrument was examined for completeness. Only two instruments were rejected based on too many incomplete or blank responses. In addition, each instrument was reviewed for consistency. Another two instruments were rejected because of inconsistent or erroneous responses.

Ponemon Institute contacted more than 200 organizations located in the United States and Canada (many with global or trans-border operations) for possible participation in this study. A total of 63 organizations participated in this research. This primary sample yielded 80 separate companies since some participating companies have stand-alone or decentralized operations.

The primary contact to these organizations was the chief security officer, the chief information security officer, the chief privacy officer or another individual who has overall responsibility for privacy & data protection. All benchmark results were gathered and analyzed by the researcher. All individual and company identifiable information was promptly deleted to protect the confidentiality of responding organizations. Field work for this research was completed in October 2009 and conducted over a four-month period.

Pie Chart 1 reports the percentage frequency of participating financial service companies by industry subsector. As can be seen, banking (32 percent) and insurance (16 percent) represent the two largest subsectors in our benchmark sample.

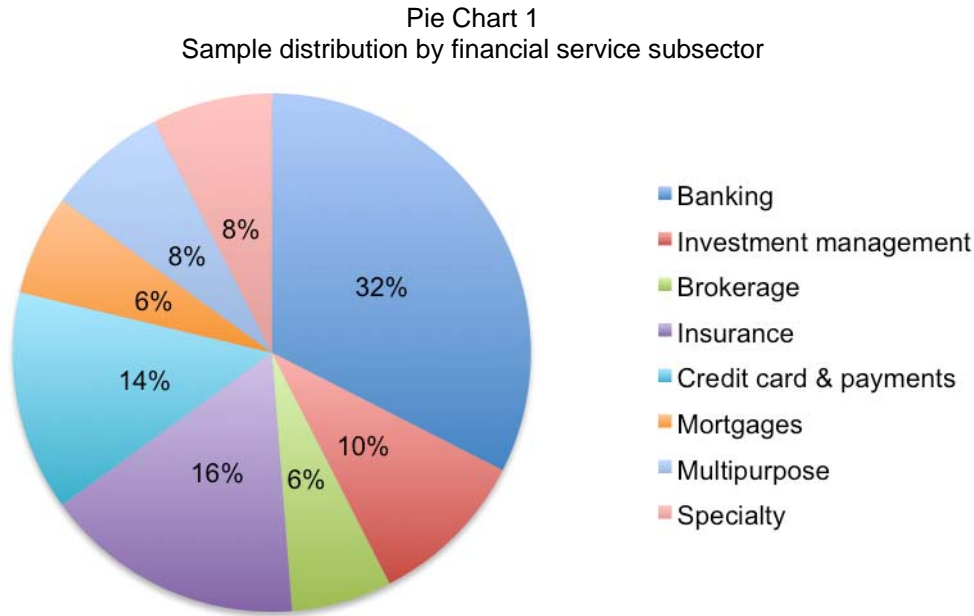
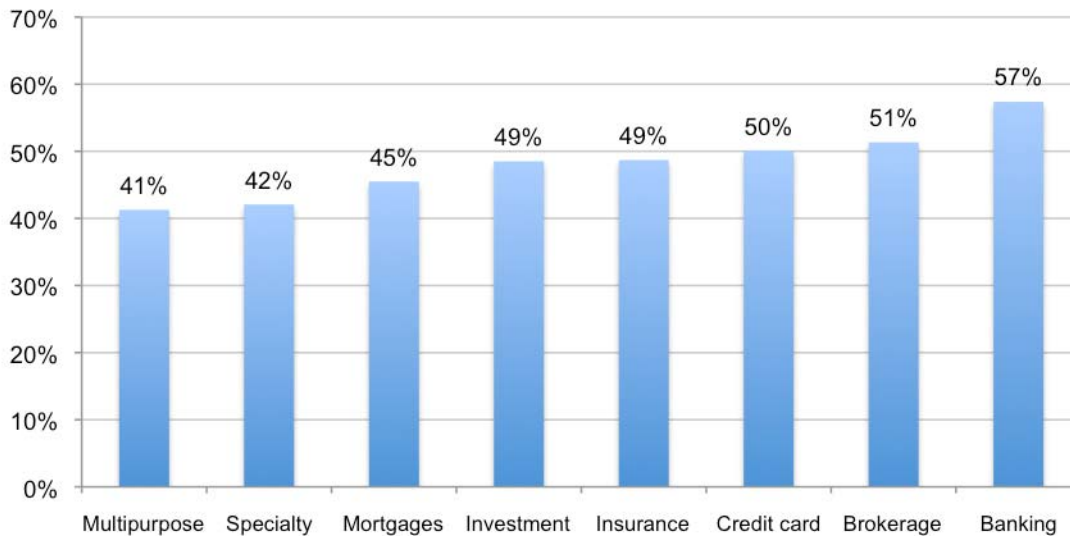


Table 2 summarizes key characteristics of participating organizations by three categories for organizational size as measured by revenues and full-time equivalent headcount.

Table 2 Sample characteristics by three levels of organizational size	Large	Medium	Small
Annual revenue	> \$20 billion	\$4 to \$20 billion	< \$4 billion
Headcount	> 25,000	5,000 to 25,000	< 5,000
Total frequency by size	27	30	23
Freq with global operations	27	16	4
Pct% with global operations	100%	53%	17%

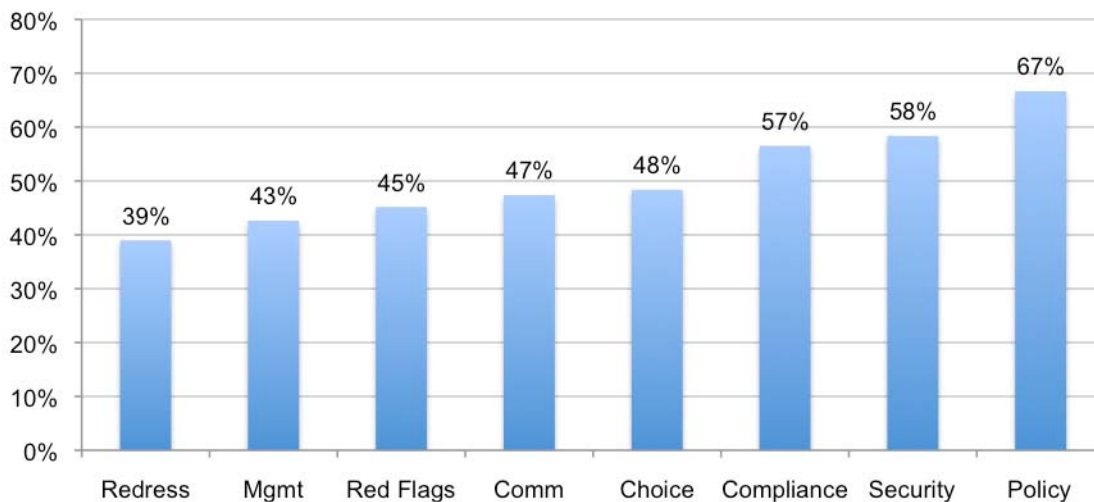
Bar Chart 8 reports the average percentage Yes scores for eight financial service sectors. As can be seen, retail banks achieve the highest average benchmark score at 57 percent yes response. Multipurpose and specialty financial service organizations have the lowest average benchmark scores at 41 and 42 percent, respectively.

Bar Chart 8
Average benchmark Yes response by financial service industry subsectors



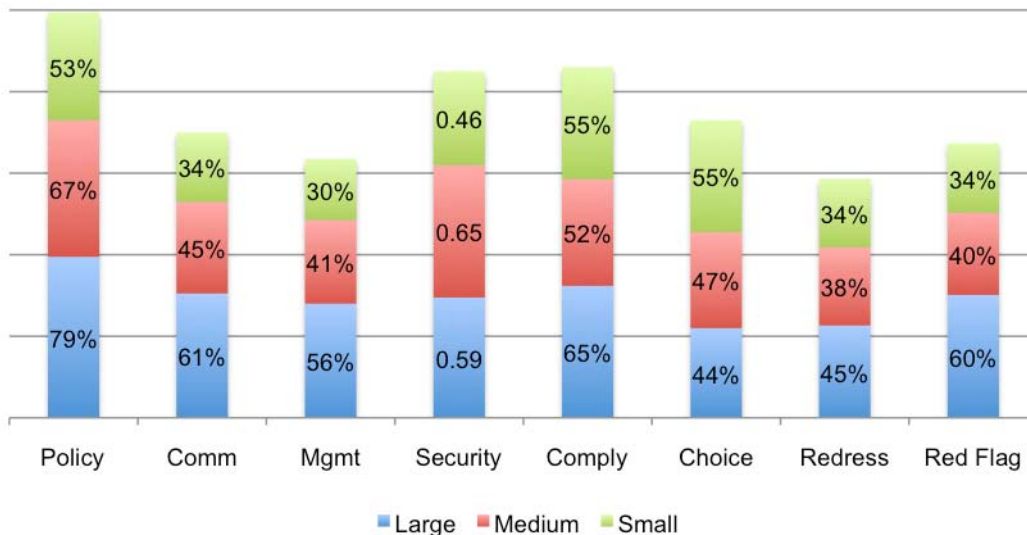
Bar Chart 9 shows the average benchmark results or Yes response for eight categories contained in the research instrument. Policy-related benchmark items achieves the highest overall score at 67 percent, while redress has the lowest average score at 39 percent.

Bar Chart 9
Average benchmark Yes response by privacy program categories



Bar Chart 10 summarizes the average benchmark score or Yes responses for eight benchmark categories and three organizational size groups (small, medium and large). As shown, larger-sized financial service organizations appear to achieve higher benchmark scores than both medium and smaller-sized companies, with one notable exception for data security where medium-sized organizations enjoy the highest average score.

Bar Chart 10
Average Yes score by benchmark category and organizational size



IV. Conclusion

Most organizations in our study have procedures and processes in place to address the risks to sensitive or confidential information. However, we found that in every organization in our study there are gaps and areas of vulnerability that put them at risk. In the beginning of the paper, we identified the six risks that can have serious financial consequences for financial institutions as well as prove damaging to reputation and customer loyalty. We recommend, therefore, that organizations take the following steps:

Data Breach Risk

- If real data is used in development and testing, take appropriate steps to safeguard the information through anonymization, masking, subsetting or other methods.
- Make sure to use encryption and to secure the network's endpoints.
- Use data loss prevention solutions to curtail the leakage of sensitive information.
- Use intrusion detection systems to safeguard sensitive information from external threats.
- Perform background checks on all privileged users (such as system administrators) and contractors before granting access to consumer, customer or employee data.

Privacy Governance

- Provide consumers with more control over their personal information. Allow them to access their personal information so they can make any necessary changes.
- Implement redress, mediation and arbitration procedures for resolving privacy concerns.
- Have in place a helpline for customers and consumers to ask questions or report a problem. The helpline should be staffed with employees who are knowledgeable about the privacy and data protection practices of the organization. This includes educating these employees on how to respond to and escalate privacy complaints.
- Make sure there is a specific timeline for investigating privacy complaints.
- Conduct privacy audits and communicate the results of these audits with senior management.
- Have procedures in place to know or understand the root causes of privacy violations or data breach incidents.

- Have sufficient records management procedures are in place to ensure that documents containing consumer or customer information can be obtained easily, especially in the event of an e-discovery request

Training and Awareness

- Assess privacy training for effectiveness.
- Make sure training is easily accessible and available on demand.

Outsourcing Sensitive Data to Third Parties

- Manage the outsourcing threat by making sure your business partners and other third parties have appropriate safeguards in place and that standard contracts contain language that ensures they will protect your data.
- Take an inventory of all locations where consumer or customer information is shared outside the organization and have signed agreements with third parties that specify the allowable retention period for sensitive data.
- Have sufficient records management procedures are in place to ensure documents containing consumer or customer information are retained according to statutory requirements and not beyond these requirements.

These steps do not guarantee that you will avoid a data breach or other privacy incident. They can serve to greatly reduce the threat to organizations in all industry sectors.

If you have questions about this report, please contact research@ponemon.org.

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 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 1: Benchmarks

The following tables summarize the audited results of an independently conducted benchmark study completed by Ponemon Institute and sponsored by Compuware. The following aggregated results present the average of 80 financial service organizations located in North America. This work was completed over a four month period ending October 2009.

The Yes percentage response is used to measure attributes that enhance an organization's privacy and data security posture. It is measured as the frequency of affirmative responses to each question divided by the frequency of completed response (i.e., the base or denominator). Certain items **highlighted in red** are reversed scored because a Yes response diminishes the organization's privacy and data security posture.

	Privacy Policy: Standard Questions	Base	Freq.	Yes%
1	Does your company have a privacy policy?	80	80	100%
2	Does your company have a separate privacy policy for employees?	74	45	61%
3	Does the company have an acceptable use policy for email and Internet?	77	45	58%
4	Does your company attempt to align its privacy policy with the expectations of regulators?	80	45	56%
5	Does your company align the privacy policy with its business conduct or ethics policy?	75	56	75%
6	Does the privacy policy address trends and issues within your industry?	71	23	32%
7	Does more than one privacy policy exist within your organization (by division, products, geographic area or function)?	79	42	53%
8	If you are a multinational company, do you have different policies for different countries?	33	23	70%
9	If multiple policies exist, is there a process in place to ensure the policies are consistent?	42	20	48%
10	Does your company have a "version control" process over privacy policies and notices?	78	61	78%
11	Does your company have formal controls over revising the privacy policy?	76	50	66%
12	Does the policy explain differences between online and off-line privacy practices?	80	49	61%
13	Does your company render a notice to customers once each year as required under the Gramm-Leach-Bliley Act? If you are not required to comply with GLBA, please note as an exception.	67	67	100%
14	Is the company's privacy policy reviewed and approved by senior executives?	80	70	88%
15	Does each Web form that captures personal information have a link to your posted privacy policy?	70	38	54%
	Average	71	48	67%

Training & Communication: Standard Questions		Base	Freq.	Yes%
16	Is the privacy policy easy to understand (written at a 10 th grade level of reading comprehension)?	70	35	50%
17	Is there a process for communicating the privacy policy and related practices to customers and consumers on a periodic basis?	77	75	97%
18	Is there a process for communicating the privacy policy to all employees who <u>interact</u> with customer data? <i>Interact means use, create, change, store, manage and destroy records about people and households.</i>	75	43	57%
19	Is there a process for communicating significant changes in the company's privacy policy to customers and consumers in a timely fashion?	75	39	52%
20	Is there a formal process for capturing feedback from customers and consumers who have additional questions about the policy or notice they receive from your company?	70	23	33%
21	Is the privacy policy posted on the Web site?	79	79	100%
22	Is the privacy policy posted at branch office locations?	74	35	47%
24	Does your company share the privacy policy or notice with its <u>business partners</u> ? <i>Business partners may include vendors, contractors, agents and outsourced relationships.</i>	75	40	53%
25	Does your company have a privacy awareness activity for new employees who interact with customer data?	75	45	60%
26	Is there an awareness or outreach effort to new customers?	75	11	15%
27	Does your company have an ongoing privacy training program that continually reinforces key concepts to all employees?	75	45	60%
28	Is the privacy training program customized by job function or information risk levels?	45	23	51%
29	Is privacy training mandatory for key employees (those who interact with customer data)?	45	22	49%
30	Is specialized training available to employees who have expanded access to customer data (including privileged users)?	45	30	67%
31	Is privacy training available to contractors and other IT vendors who have access to personal information about customers, consumers, employees and so forth?	45	13	29%
32	Is the privacy training program assessed for effectiveness?	45	12	27%
33	Is training available to employees on demand (such as CBT or video program)?	45	14	31%
34	Are the results of privacy training communicated to the company's privacy leader or other senior executives?	45	7	16%
35	Are the results of the company's privacy program communicated to the Board of Directors (or Audit Committee)?	45	3	7%
	Average	62	31	47%

Privacy Management: Standard Questions		Base	Freq.	Yes%
36	Does your company have a privacy leader such as a Chief Privacy Officer (CPO) responsible for the privacy program? If no, skip all items highlighted in yellow.	75	45	60%
37	Does the privacy leader report directly to senior management?	45	22	49%

38	Is the privacy leader fully dedicated to the privacy program (e.g., is it a full-time job)?	45	23	51%
39	Does the privacy leader have a lead role on a cross-functional committee?	45	23	51%
40	Does your company have privacy coordinators or liaisons to support program goals at the business unit level or by geographic locations?	70	21	30%
41	Does the privacy program have sufficient resources to achieve its objectives?	80	40	50%
42	Does your organization have a privacy steering committee composed of individuals from different functions, departments or information users? If no, skip all items highlighted in green.	79	46	58%
43	Does the privacy steering committee have a set of formal responsibilities including a charter?	46	21	46%
44	Does your organization have sufficient procedures (SOPs) or guidance to manage the privacy program effectively?	73	39	53%
45	Does your organization perform reviews (vetting procedures) of business partners* before sending them personal information about customers, consumers, employees and others?	80	39	49%
46	Do standard contracts with business partners* contain language that ensures privacy protections?	77	38	49%
47	Has an independent privacy audit been conducted in the past two years?	76	23	30%
48	Are there follow-up procedures to take corrective action following an audit or review?	76	47	62%
49	Is there a formal process for determining key managers' compliance with privacy policy?	76	20	26%
50	Does the company comply with a major privacy and/or security seal program?	73	21	29%
51	Does the company have sufficient records management procedures to ensure that documents containing consumer or customer information can be obtained easily (for example, in the event of an e-discovery request)?	73	30	41%
52	Do you have an inventory of all locations that you share your consumer or customer information outside your organization (examples may include printing vendors, credit bureaus, affiliates)?	70	11	16%
53	Do you have signed agreements on the allowable retention period for outside entities that have your consumer or customer information?	69	13	19%
54	Does the company have sufficient records management procedures to ensure that documents containing consumer or customer information are retained according to statutory requirements (not beyond these requirements)?	71	29	41%
	Average	68	29	43%

	Security: Standard Questions	Base	Freq.	Yes%
55	Does your company have a data protection strategy or plan?	80	61	76%
56	Do you have an inventory of all applications and technologies that use consumer or customer information?	77	21	27%
57	Do you use technologies or other means to identify unauthorized or illegal movement or transfer of data or documents?	79	69	87%
58	Do you use technologies or other means to prevent unauthorized or illegal movement or transfer of data or documents?	79	69	87%
59	Does the company capture Social Security numbers of customers for identification and/or authentication purposes?	77	68	12%
60	Does the company take steps to secure the use of Social Security numbers such as special policies for handling this data or visually blocking SSN from user/operator views?	68	60	88%
61	Does the company attempt to classify or categorize personal information by sensitivity, confidentiality or risk levels?	77	60	78%
62	Does the company use dual authentication methods to limit or control access to sensitive or confidential information (e.g., see FFIEC guidelines)?	76	60	79%
63	Does the company use of, customer or employee information in development and testing?	71	59	17%
64	Does the company take appropriate steps to protect real data used in development and testing such as anonymizing, masking, subsetting or other methods?	59	29	49%
65	Are HTML crawling or sniffing technologies used to determine privacy compliance on Web sites?	70	39	56%
66	Does your company's Web site deploy the Platform for Privacy Preferences (P3P compact or full XML policy)?	70	3	4%
67	Does your company attempt to control all domains linked to your company's primary Web domain?	71	32	45%
68	Does your company's IT security team review Web site content for privacy compliance before publication?	73	40	55%
69	Are new software applications and databases reviewed for privacy considerations and compliance to law before placed into production?	75	35	47%
70	Are persistent cookies used on your company's Web site?	75	41	45%
71	Are Web beacons used on your company's Web site?	75	46	39%
72	Does your company conduct identity compliance procedures to ensure that user access rights are accurate, complete and appropriately specified to fulfill a given set of business functions?	70	39	56%
73	Are data storage devices operated in physically secure areas?	80	65	81%
74	Are there physical security safeguards that prevent access to storage devices containing consumer or customer information?	78	69	88%
75	Does your organization utilize data loss prevention (DLP) solutions to curtail the leakage of consumer or customer information?	71	29	41%

76	Are there security safeguards, such as whole disk encryption, to prevent consumer or customer data on laptop computers or other portable devices from being lost or stolen?	75	38	51%
77	Are endpoints to the company's network or enterprise system sufficiently secured?	75	23	31%
78	Is information security integrated with privacy compliance?	71	20	28%
79	Does your company use Secured Socket Layer (SSL) on all Web forms containing sensitive personal information?	71	65	92%
80	Does your company authenticate visitors to <u>all</u> of your Web sites that contain sensitive or confidential information?	71	60	85%
81	Does your company use authentication to determine who has access to personal information?	71	53	75%
82	Does your company use encryption in the exchange of customer information?	72	63	88%
83	Does your company use encryption in securing information in storage?	71	60	85%
84	Does your company have multilayered firewall protection over consumer or customer data?	79	79	100%
85	Are background checks performed on all privileged users (such as system administrators) and contractors before they are granted access to consumer, customer or employee data?	72	40	56%
86	Does your company have intrusion detection systems (IDS)?	72	34	47%
87	Does your company monitor for malware upon the downloading of software or in launching new Web content?	72	41	57%
88	Are laptops or other mobile data-bearing devices given access to the company's network or mainframe system through insecure channels?	72	50	31%
89	Are backup tapes and other media encrypted (prior to transmission or movement to archive)?	71	36	51%
90	Are business partners* required to comply with reasonable security protection practices?	75	53	71%
	Average	73	47	58%

	Privacy Compliance & Monitoring: Standard Questions	Base	Freq.	Yes%
91	Are mock regulatory assessments (a.k.a. fire drills) conducted to determine compliance with policy or law?	80	10	13%
92	Do you monitor the company's internal compliance to the company's privacy policy on an ongoing basis?	80	69	86%
93	Are mystery shopping techniques used to test privacy "readiness" of customer services (call centers)?	80	9	11%
94	Is monitoring of privacy compliance conducted by internal auditors (or other auditing professionals)?	78	69	88%
95	Does the privacy leader report the results of compliance to the Board?	45	12	27%
96	Is senior management supportive of the privacy program?	80	55	69%
97	Is privacy and data protection a significant concern for the company?	80	41	51%
98	Does your company monitor insider threats such as negligence or malicious employees?	77	65	84%
99	Does your company utilize surveillance methods for Internet and email of employees?	65	55	85%
100	Does your company attempt to ensure that marketing programs and campaigns are privacy compliant?	70	23	33%
101	Does your company utilize employee surveillance methods?	65	55	85%
102	Does your company inform employees that surveillance is being conducted?	55	32	58%
103	Does your company monitor emerging state, federal and global privacy regulations?	73	63	86%
104	Does your company have a formal crisis management process for privacy violations or data breaches?	75	59	79%
105	Does your company self-report privacy violations to regulatory authorities?	75	56	75%
106	Has the company experienced significant privacy violations or data breach incidents within the recent past?	75	38	49%
107	Does your company have sufficient procedures to know or understand the root causes of most privacy violations or data breach incidents?	70	29	41%
108	Does the internal audit or compliance department conduct ongoing privacy assessments?	80	46	58%
109	Do you inventory your data to assess the collection, use and sharing of personal information?	78	19	24%
110	Does the company monitor access rights and privileges, such as revoking access rights when employees or temporary employees are terminated?	78	59	76%
111	Do you have contract employees that have access to sensitive data?	75	68	9%
	Average	73	44	57%

	Choice & Consent: Standard Questions	Base	Freq.	Yes%
112	Does your company provide choice to customers before sharing information with affiliates	80	18	23%
113	Does your company provide choice to customers before sharing information with non-affiliated third parties?	74	54	73%
114	Does your company provide choice to different message delivery channels (email, telephone, mail, Internet)	77	23	30%
115	Does your company provide multiple (more than one) methods for customers to express privacy preferences?	80	11	14%
116	Does your company perform tests to determine if consent or choice is being honored?	75	26	35%
117	Does your company monitor marketing activities that use permission-based lists?	71	19	27%
118	Does your company provide "opt out" over the secondary uses of personal information?	79	34	43%
119	Does the company provide adequate details on how customer information will be used and shared?	80	67	84%
120	Does the company's commercial outbound email provide an unsubscribe feature?	78	74	95%
121	Is there flexibility in the way consumers and customers can communicate their privacy choice, consent or preference? If no, skip all items highlighted in yellow.	78	35	45%
122	Does your company allow consumers and customers to communicate their privacy choices by registering on a Web site?	35	23	66%
123	Does your company allow consumers and customers to communicate their privacy choices by telephone to a customer services?	35	24	69%
124	Does your organization participate in any level of behavioral tracking or marketing?	69	50	28%
	Average	70	35	48%

	Redress & Enforcement: Standard Questions	Base	Freq.	Yes%
125	Can customers and consumers access in order to view and correct their personal information?	75	19	25%
126	Do customers and consumers have access to a redress procedure for resolving privacy concerns?	75	18	24%
127	Does the company provide mediation or arbitration on privacy matters?	80	21	26%
128	Do customers have access to the company's privacy leader?	45	5	11%
129	Is the redress process clearly described in the privacy notice or policy?	77	50	65%
130	Does the company have a help line for customers and consumers to ask questions or report a problem about privacy?	77	25	32%
132	Does the company have a standardized process for responding to help line calls?	25	10	40%
133	Does the company educate call center employees on how to respond and escalate privacy complaints?	71	18	25%
134	Does the company have a specific timeline for investigating alleged privacy complaints?	75	11	15%
135	Does the company have a formal procedure for enforcing privacy violations or known abuses?	77	39	51%
136	Does the redress process have specific reporting requirements to management?	75	8	11%
137	Does the company have a formal process for reporting privacy or security breaches to data subjects involved in the breach?	75	49	65%
138	Does the company have a formal process to self report privacy or security breaches to regulatory authorities?	75	43	57%
139	Has the company undergone a regulatory inquiry or review for privacy within the recent past?	59	38	36%
140	Has the company experienced a privacy violation that was reported in the media?	69	19	72%
	Average	68	26	39%

	Red Flags Rule: Standard Questions	Base	Freq.	Yes%
141	Does your organization have a Red Flags Rule program in-place?	80	69	86%
142	Do you have employees responsible for ensuring compliance with the Red Flags Rules?	69	40	58%
143	Is your Red Flags Rule program coordinated across the enterprise?	69	45	65%
144	Do you perform risk assessments to determine how different operations within your organization will be affected by Red Flag Rule requirements?	69	30	43%
145	Have your know-your-customer policies been modified to comply with the Red Flags Rule?	69	23	33%
146	Have you implemented an education and awareness program to ensure employee compliance with the Red Flags Rule?	69	35	51%
147	Have security systems been reviewed and possibly modified to ensure compliance with the Red Flags Rule?	69	20	29%
148	Have you taken steps to reduce the collection of unnecessary sensitive customer information in order to curtail identity theft?	68	19	28%
149	Have you expanded use of third-party fraud alerts on customer accounts?	68	39	57%
150	Have you expanded use of cyber crime alerts from law enforcement or government?	68	38	56%
151	Do you have controls over paper documents containing protected customer information?	69	30	43%
152	Have you implemented redress procedures for customers who are concerned about becoming an identity theft victim?	69	21	30%
153	Have you implemented new or revised method for tracking customer complaints that relate to concerns about identity theft?	68	12	18%
154	Do you have procedures for promptly contacting law enforcement in the event an identity theft is believed to have occurred?	69	38	55%
155	Have you designated a responsible person in each local office or branch operation to ensure compliance with the Red Flags Rule program?	67	16	24%
	Average	69	32	45%