

Sponsored by



Independently Conducted by



**Presents**

# **Privacy Breach Index Survey: Executive Summary**

**Presented by Ponemon Institute LLC**

**August 19, 2008**

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 Please Do Not Quote Without Express Permission.**



## Privacy Breach Index Survey

Executive Summary by Larry Ponemon, August 19, 2008

With the occurrence of thousands of data breaches and more than 200 million records containing personal information lost or stolen since January 2005, no longer is it considered a matter of *if* your organization will have a data breach but *when* your organization will have an incident. So when the fateful day arrives, will your company have a quality privacy incident response plan in place? Will you be able to measure its effectiveness and make the necessary improvements to better safeguard sensitive information from a future breach?

Sponsored by Hilb Rogal & Hobbs, Ponemon Institute created a benchmarking tool called the Privacy Breach Index (PBI)<sup>™</sup> to measure the quality of companies' response to a data loss or theft, especially when it concerns information about people and their families. The Privacy Breach Index (PBI) benchmark tool can assist companies to do the following:

- Improve existing procedures and safeguards for prevention of a data breach.
- Determine areas where an organization is most vulnerable to a data breach.
- Benchmark your organization's response to a data breach against other companies.

The PBI is compiled from surveys completed by 768 individuals in the data protection, IT security and compliance professions who have the expertise or experience to assess their organizations' quality of response following an organization's breach incident. Each participant in the survey self-reported that their organization had a data breach involving the loss or theft of customer, consumer or employee data in the past 24 months.

The PBI survey questions address the core activities that encompass all aspects of a company's data loss incident response, such as: detection and forensics, escalation to management, notification quality and timeliness to breach victims, support to breach victims (such as credit monitoring or identity theft protection), post-mortem response, reputation management and response to regulatory or legal action.

The results of the PBI study provide further evidence of the importance of having a good quality privacy incidence response plan in place. More than 83% of respondents believe that the individuals affected by the data breach lost trust and confidence in their organization's ability to protect their personal information. As we have found in our consumer studies on trust, these perceptions often result in the loss of customer loyalty. In fact, 80% of respondents in the PBI study reported that a certain percentage of data breach victims terminated their relationship with the organization.

The following are five key findings from the survey:

1. Only 9% of respondents gave an "A" or excellent to their organization's overall performance in responding to their organizations' most recent data breach incident. Thirty-one percent said their performance rated a "B" or good and 26% said it rated a "C" or fair grade. While 29% gave a "D" or poor and 5% gave their organization an "F" for failure.
2. An overwhelming 80% of respondents believe that their organizations experienced some loss of customers or other data breach victims after the incident.
3. The number one root cause of data breach incidents reported by participants is employee negligence (50% of participants) followed by third party negligence (29%). External penetration (hackers) was low at 3% and other criminal activity was only 1%.

4. Most respondents say their companies have had multiple data breaches. More than 36% of respondents have between one and four data breach incidents involving 100 or more records each year, 32% have between five and eight and 31% have nine or more incidents.
5. Respondents believe that the ex-post response to a data breach (such as conducting an assessment after the incident is closed) and detection and escalation of the incident (such as ensuring that third parties are instructed to inform your organization if they have a data breach involving your organizations' sensitive and confidential data) are very important or important to a successful privacy incidence response plan.

### Privacy Breach Index Benchmark Responses

Participants in the study were asked to indicate whether or not their companies' privacy breach response plan included specific activities in four categories (prevention, detection & escalation, notification and ex-post response) and to rank the importance of these activities in helping them manage the data breach they experienced in the past 24 months.

The two dependent variables in this research are the percentage Yes response to each benchmark item and the relative importance of this benchmark item to the management of the data breach incident. Following is the scale used to calculate the relative importance of each item receiving a Yes response within the benchmark instrument:

- +2 = Item is very important
- +1 = Item is important
- 0 = Item is net neutral
- -1 = Item is not important
- -2 = Item is irrelevant

Hence, an absolute *perfect* score would mean everyone completing the survey assigned +2 to the item and the absolute *imperfect* score would mean that everyone assigned -2 to the item. Most items yielded positive results, suggesting an item mean above zero (i.e., more positive than negative scores).

In general, the findings from the benchmark study reveal an interesting gap between the practices companies currently have in place to respond to an incident and those practices that are not in place yet could be critical in addressing the data breach. The following describes the most salient findings from our survey.

### Activities that are both widely used in companies and most effective in responding to the breach:

- Strong authentication measures for granting employees and contractors access to its information systems (59% Yes score; 0.63 Importance score).
- Prompt change of physical and electronic access rights of employees when they change jobs or are terminated (62% Yes score; 0.64 Importance score).
- Organization's privacy leader is involved in the detection and escalation process (50% Yes score; 0.80 Importance score).
- There is a process for restricting the release of information about the data breach incident (62% Yes score; 0.56 Importance score).
- There is full documentation of the incident response from initial discovery to disclosure (72% Yes score; 1.03 Importance score).

- There is a process for ensuring that communication about the breach is kept confidential until the company notifies victims and other stakeholders (50% Yes score; 0.72 Importance score).
- A communications plan for employees who are responsible for responding to data breach victims (51% Yes score; 0.64 Importance score).
- Policies describing how personal information should be protected from being lost or stolen (91% Yes score; 0.59 Importance score).

**Activities most widely used but not considered effective in responding to the breach include:**

- Secure physical locations where personal information is stored (89% Yes score; -0.02 Importance score).
- Regular monitoring of information systems for unusual traffic flow or other activity (72% Yes score; 0.34 Importance score).
- Employees have the ability to report data protection risks that might result in a data breach to appropriate supervisors or management personnel (88% Yes score; -0.38 Importance score).
- There is an existing contact channel (letter, email, phone call) to communicate with the data breach victim (64% Yes score; 0.15 Importance score).
- There is a function or leader responsible for managing the data breach incident (51% Yes score; 0.45 Importance score).

**Activities not widely used but should be a part of a data breach response plan.**

- Conduct periodic risk assessments of third parties, vendors or business partners that have access to its personal information (28% Yes score; 0.91 Importance score).
- Dispose of data-bearing devices containing personal information in a secure manner. (19% Yes score; 0.85 Importance score).
- Instruct third parties, including contractors and business partners on how to inform your organization when they have a data breach involving your company's sensitive personal information (19% Yes score; 0.84 Importance score).
- A process for ensuring that all communications are done according to a pre-determined timeline (42% Yes score; 0.79 Importance score).
- A communications plan for notifying the media (39% Yes score; 0.68 Importance score).
- An assessment, audit or post-mortem procedure is required after the incident is closed (36% Yes score; 1.30 Importance score).
- A process to make recommendations for improvement (37% Yes score; 1.21 Importance score).
- A process to implement recommendations for privacy and data protection risk assessment programs (42% Yes; 0.72 Importance score).
- A process to determine responsibility for the data breach incident (48% Yes; 0.78 Importance score).



- A process for verifying that contact with each data breach victim has been completed (39% Yes; 0.69 Importance score).

The findings described above indicate that many companies are at a nascent stage in their privacy breach response plans. We believe an important benefit of the PBI will be to help companies learn where they should be allocating resources to better respond to a breach and address the current areas where they are most vulnerable to an incident.

The PBI survey will be available for download from [www.privacybreachindex.com](http://www.privacybreachindex.com). For a fee, companies that complete the PBI benchmark instrument will receive a customized report that compares their response to a breach incident to the companies and industries in the PBI index. The report will provide the company with a performance measure or “score” and guidance on how it can improve the core activities associated with responding to a data loss incident.

### **Study Availability**

A copy of the Privacy Breach Index™ Executive Summary and a questionnaire that can be used to create a company’s PBI score are both available for download via the following link: [www.privacybreachindex.com](http://www.privacybreachindex.com). For specific questions about the Privacy Breach Index™, please contact Paul Paray at [paul.paray@hrh.com](mailto:paul.paray@hrh.com) or 212-907-5934. Further information regarding HRH’s Network Security & Privacy Advisory Group can be found at [www.hrh.com/privacy](http://www.hrh.com/privacy).

### **About Hilb Rogal & Hobbs**

Hilb Rogal & Hobbs Company (HRH) is the eighth largest insurance and risk management intermediary in the United States and the world, with over 140 offices around the globe. HRH helps clients manage their risks in property and casualty, employee benefits, professional liability and other areas of specialized exposure. In addition, HRH offers a full range of personal and corporate financial products and services. HRH is focused on understanding our clients' businesses, employees and risks, as well as the insurance and financial markets, so that we can develop insurance, risk management and employee benefits solutions that best fit their needs. The company's common stock is traded on the New York Stock Exchange, symbol HRH. More information about HRH may be found at [www.hrh.com](http://www.hrh.com).

### **About the Ponemon Institute**

The Ponemon Institute is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries. More information and Ponemon Institute may be found at [www.ponemon.org](http://www.ponemon.org).



# 2008 Privacy Breach Index Survey

Final Document Prepared by Dr. Larry Ponemon

Dear Participant,

Has your organization provided notification of a data breach? If you sent notification about the loss or theft of personal information entrusted to you, were you satisfied with the steps your organization took to complete the incident response process? The first two parts of this survey focuses on how well you believe your organization responded to a recent data breach. Part three asks how important you believe certain attributes are in preventing and responding to a data breach.

We appreciate your frank responses to all survey questions. Please be assured that we will not collect any personally identifiable information. If you have any questions, contact Ponemon Institute at [research@ponemon.org](mailto:research@ponemon.org) or call us at 1.800.887.3118.

Thank you in advance for your participation.

*L.A. Ponemon*

Dr. Larry Ponemon  
Chairman

## Key definitions

Data breach victim is defined as the individual or household receiving notification that their personal information was either lost or stolen.

Personal information is information about a natural person, household or family. This information includes name, address, telephone numbers, e-mail address, Social Security number, other personal identification numbers, access codes, age, gender, income and tax information, shopping information, account activity and any other sensitive pieces of data about an individual.

## Part 1: Screening questions

S1. Did your organization experience a data breach involving the loss or theft of customer, consumer or employee data in the past 24 months?

- Yes
- No (**STOP**)

S2. If yes, were you required to notify **data breach victims** whose information was lost or stolen?

- Yes
- No (**STOP**)

S3. If yes, under what statute(s) or regulation(s) were you required to notify data subjects that their information was lost or stolen?

- GLBA
- HIPAA
- OCC
- State Statutes
- Other (please specify)



**Part 2: Please respond to all questions based on your most recent incident requiring data breach notification.**

Q1. What type of personal information was lost or stolen in this breach incident?

- Customer or consumer information
- Employee, temporary employee or contractor information
- Other (please specify)

Q2, What was the root cause of this data breach incident?

- Employee negligence
- Third-party negligence
- Malicious employees
- External penetration (hack)
- Other criminal activity
- Do not know

**What was the condition of your organization’s privacy and information security ecosystem at the time the data breach incident occurred?**

Please answer all questions A1 to A14 based solely on your organization’s response to its most recent data breach incident.

The following fourteen (14) attributes define the quality and effectiveness of an organization’s response to data breach. Please rate your organization’s response to its data breach incident using the 10-point scale provided below each attribute.

- 1 ≡ Lowest – at the time of the breach this attribute did not exist or was poorly managed.
- 10 ≡ Highest – at the time of the breach this attribute was managed effectively.

A1. Availability of an incident response plan for data breach

1	2	3	4	5	6	7	8	9	10

A2. Availability of forensic support

1	2	3	4	5	6	7	8	9	10

A3. Thoroughness of detection

1	2	3	4	5	6	7	8	9	10

A4. Complete understanding of legal requirements

1	2	3	4	5	6	7	8	9	10

A5. Accurate identification of individuals requiring notification

1	2	3	4	5	6	7	8	9	10

A6. Containment of information about the breach to those who had a need to know

1	2	3	4	5	6	7	8	9	10

A7. Minimization of harms

1	2	3	4	5	6	7	8	9	10

A8. Timely notification or disclosure to **data breach victims**

1	2	3	4	5	6	7	8	9	10

A9. Access to experts and knowledgeable legal counsel

1	2	3	4	5	6	7	8	9	10

A10. Efficient management of organization's resources

1	2	3	4	5	6	7	8	9	10

A11. Ability to manage media relations and reporting of the incident

1	2	3	4	5	6	7	8	9	10

A12. Thorough post-mortem with full documentation and audit trail

1	2	3	4	5	6	7	8	9	10

A13. Upward communication to senior management

1	2	3	4	5	6	7	8	9	10

A14. Comprehensive remediation

1	2	3	4	5	6	7	8	9	10



Q3. In your opinion, did victims lose trust and confidence in your organization's ability to protect their personal information?

- Yes
- No

Q4. Approximately, what percentage of **data breach victims** decided to terminate their relationship with your organization as a result of this incident?

- Zero
- Between 1 to 5%
- Between 6 to 10%
- Between 11 to 15%
- More than 15%

Q5. Approximately, how many data breach incidents involving 100 or more records does your organization experience each year?

- Less than one incident
- Between 1 to 2 incidents
- Between 3 to 4 incidents
- Between 5 to 6 incidents
- Between 7 to 8 incidents
- Between 9 to 10 incidents
- More than 10 incidents

Q6. In your opinion, what grade would you assign to your organization's overall performance in responding to the data breach incident?

- A = Excellent
- B = Good
- C = Fair
- D = Poor
- F = Failure



**Part 3: Privacy Breach Index questions.** Please answer each question listed below with a Yes, No or Unsure response. For Yes responses, please rate the importance of each control activity from very important to irrelevant.

		Yes/No/Unsure	Very important	Important	Sometimes important	Not important	Irrelevant
	<b>Prevention:</b> For each “yes” response to the following questions, please rate the importance of the control activity.						
1	Does your organization have policies describing how personal information should be protected from being lost or stolen?						
2	Does your organization have a training and awareness program available to customer service employees who might receive questions about privacy and data protection practices?						
3	Does your organization promptly change physical and electronic access rights of employees when they change jobs or are terminated?						
4	Does your organization practice strong authentication measures for granting employees and contractors access to its information systems?						
5	Are employees’ mobile devices (i.e. laptops, PDAs, cell phones) encrypted?						
6	Is the transmission of sensitive personal information encrypted?						
7	Does your organization regularly monitor its information systems for unusual traffic flow or other activity?						
8	Does your organization secure physical locations where personal information is stored?						
9	Are operating systems, applications and databases where data is stored and transmitted secured against intrusion?						
10	Do your employees have the ability to report data protection risks that might result in a data breach to appropriate supervisors or management personnel (upward communication)?						
11	Does your organization verify that its privacy and security procedures can prevent a data breach?						
12	Does your organization conduct periodic risk assessments to determine where personal information is vulnerable to a data breach?						
13	Does your organization conduct periodic risk assessments of third parties, vendors or business partners that have access to its personal information?						
14	Are these risk assessments used to improve the security of sensitive or confidential information in your organization?						
15	Are data-bearing devices containing personal information disposed of in a secure manner?						

		Yes/No/Unsure	Very important	Important	Sometimes important	Not important	Irrelevant
	<b>Detection &amp; Escalation:</b> For each “yes” response to the following questions, please rate the importance of the control activity.						
16	Is there a process in place to determine the potential harms experienced by victims as a result of the breach?						
17	Is there a function or leader responsible for managing the data breach incident?						
18	Has your organization established a cross-functional incident response team?						
19	Does your organization have enabling technology (such as DLP) to monitor potential data breaches?						
20	Are employees informed about how to report a data breach within the organization (upward communication)?						
21	Is there a process for restricting the release of information about the data breach incident (e.g., on a need to know basis only)?						
22	Are third parties, including contractors and business partners, instructed on how to inform your organization when they have a data breach involving your company's sensitive personal information?						
23	Does your organization have a special team assigned to investigate a data breach incident?						
24	Does your organization have internal specialized forensic tools and techniques in place to investigate a data breach?						
25	Is your organization's privacy leader involved in the detection and escalation process?						
26	As part of the assessment or forensic investigation, are conclusions developed, reviewed and approved by management?						
27	Are there standard operating procedures or protocols established for communicating relevant and appropriate information to law enforcement in the event of data theft or other criminal activity involving the breach incident?						

		Yes/No/Unsure	Very important	Important	Sometimes important	Not important	Irrelevant
	<b>Notification:</b> For each “yes” response to the following questions, please rate the importance of the control activity.						
28	Does your organization have a communications plan for notifying all appropriate regulatory authorities and law enforcement?						
29	Does your organization have a communications plan for notifying the media?						
30	Does your organization have a communications plan for employees who are responsible for responding to data breach victims?						
31	Does your organization have internal customer service and call center employees who respond to data breach victims' questions?						
32	Is there an existing contact channel (letter, email, phone call) to communicate with the data breach victim?						
33	Is there a process for verifying that contact with each data breach victim has been completed?						
34	Is there a process for managing incomplete or failed notification and contact returns?						
35	Is there a repository of standardized and approved communications available for use in advance of the incident?						
36	Is there a mechanism for receiving and tracking feedback about the quality and responsiveness of the organization to data breach victims?						
37	Is there a process for addressing special circumstances (i.e., disgruntled victims that require escalated management attention)?						
38	Is there a process for differentiating victims based on their personal information and accompanying exposure to ID theft or criminal activity?						
39	Is there a process for ensuring that all communications are done according to a pre-determined timeline?						
40	Is there a process for ensuring that communication about the breach is kept confidential until the company notifies victims and other stakeholders?						
41	Does your organization provide a website or link on your website for data breach victims to learn more about the data breach incident and remedies available to them?						
42	Does your organization provide free or subsidized identity protection services, including credit monitoring, to minimize harm to data breach victims?						

43	Does your organization offer more than one year of free credit monitoring to data breach victims?						
44	Is there some outreach effort to communicate the benefits of identity protection services to data breach victims?						
45	Does your organization purchase specialized insurance to reimburse for loss related to a data breach event?						
46	Does your organization fully document the incident response from initial discovery to disclosure?						
47	Is there subsequent communication or disclosure to data breach victims when new information about the breach event comes available?						

		Yes/No/Unsure	Very important	Important	Sometimes important	Not important	Irrelevant
<b>Ex-post Response:</b> For each “yes” response to the following questions, please rate the importance of the control activity.							
48	Is there an assessment, audit or post-mortem procedure required after the incident is closed?						
49	Is there a final report to senior management or the board of directors?						
50	Is there a performance review of the incident response team conducted by management?						
51	Is there a process to make recommendations for improvement?						
52	Is there a training program for those who were responsible for the breach?						
53	Does your organization attempt to calculate the cost of the data breach?						
54	Is there a process to implement recommendations for privacy and data protection risk assessment programs?						
55	Is there a process to determine responsibility for the data breach incident?						
56	Is there a process to determine appropriate actions and enforcement for non-compliance with policies?						

## Part 4: Organization characteristics and respondent demographics

Your current title is: \_\_\_\_\_

What organizational level best describes your current position?

- Senior Executive
- Vice President
- Director
- Manager
- Associate/Staff
- Other (please describe)

Check the **Primary Person** you or your supervisor reports to within your organization.

- CEO/Executive Committee
- Chief Financial Officer
- Chief Information Officer
- Compliance Officer
- Chief Privacy Officer
- Director of Internal Audit
- General Counsel
- Chief Technology Officer
- Human Resources VP
- Chief Security Officer
- Chief Risk Officer
- Other (please describe)

Check the country or U.S. region where your company's **primary** headquarters is located.

If in the United States, what state? [pull down]

If outside the United States, please provide the name of the country: [pull down]

Educational and career background:

Total years of business experience: \_\_\_years

Total years in IT or data security: \_\_\_years

Total years in current position: \_\_\_years

- Compliance (auditing, accountant, legal)
- IT (systems, software, computer science)
- Security (law enforcement, military, intelligence)
- Other non-technical field
- Other technical field

What is the approximate size of your IT department in terms of full-time equivalent (FTE) headcount?

- Less than 10 people
- Between 10 to 50 people
- Between 50 to 100 people
- Between 100 to 500 people
- Between 500 to 1,000 people
- Between 1,000 to 2,000 people
- Over 2,000 people

What industry best describes your organization's industry concentration or focus?

- Airlines
- Automotive
- Agriculture
- Brokerage
- Cable
- Chemicals
- Credit Cards
- Defense
- Education
- Entertainment
- Services
- Health Care
- Hospitality & Leisure
- Manufacturing
- Insurance
- Internet & ISPs
- Government
- Pharmaceutical
- Professional Services
- Research
- Retail
- Banking
- Energy
- Telecommunications
- Technology & Software
- Transportation
- Wireless

Other (please specify): \_\_\_\_\_

What best describes your role in managing privacy and data protection risks within your organization? Check all that apply.

- Setting priorities
- Managing budgets
- Selecting vendors and contractors
- Determining privacy and data protection strategy
- Evaluating program performance

What is the worldwide headcount of your organization?

- Less than 500 people
- 500 to 1,000 people
- 1,001 to 5,000 people
- 5,001 to 25,000 people
- 25,001 to 75,000 people
- More than 75,000 people



Thank you for your participation. All responses are completely confidential.  
Please contact [research@ponemon.org](mailto:research@ponemon.org) or call us at 800.877.3118 if you have any questions.

### **Ponemon Institute**

*Advancing Responsible Information Management*

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