PGP® Research Study – Summary

October 2006

2006 Annual Study: Cost of a Data Breach

Understanding Financial Impact, Customer Turnover, and Preventative Solutions

A study summarizing the actual costs incurred by 31 organizations that lost confidential customer information and had a regulatory requirement to publicly notify affected individuals.

Benchmark research conducted by

Ponemon Institute, LLC

The information in this document is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors.

Changes to this document may be made at any time without notice.

Table of Contents

EXECUTIVE SUMMARY 2

INTRODUCTION 5

STUDY OVERVIEW 6

STUDY METHODOLOGY 7

KEY REPORT FINDINGS 7

DATA BREACH COSTS BY CATEGORY 15

REPORT CONCLUSIONS 18

PGP SOLUTIONS 19

VONTU SOLUTIONS 20

APPENDIX A – SURVEY METHODOLOGY 23

BENCHMARK METHODS 23

Executive Summary

Customer Notification Requirements

Regulations in more than half of all U.S. states require that customers be notified if their confidential or personal data has been lost, stolen, or compromised. The only "safe harbor" exception, exempting organizations from the notification requirement, is for data held in an encrypted form when lost. When a regulatory breach occurs, organizations must notify all affected customers, attempt to minimize downstream brand consequences, and put solutions in place to prevent a recurrence.

The frequency of lost customer information is on the increase. Since February 2005, the Privacy Rights Clearinghouse has identified more than 93 million records of U.S. residents that have been exposed due to security breaches. New disclosures occur every week, and websites track these for the media and interested parties (www.privacyrights.org/ar/chrondatabreaches.htm).

2006 Annual Survey: Cost of a Data Breach

This 2006 Ponemon Institute benchmark study, sponsored by Vontu, Inc., and PGP Corporation, examines the costs incurred by 31 companies after experiencing a data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. This is the second annual survey of this issue; the first survey was published in November 2005 and is available on the PGP website (registration required): http://www.pgp.com/downloads/research_reports/index.html.

Breaches included in the survey ranged from 2,500 records to 263,000 records from 15 different industry sectors and cover the costs resulting from 815,000 compromised customer records.

Among the study's key findings:

- **Total costs:** averaged $182 per lost customer record, an increase of 30 percent over 2005 results. The average total cost per reporting company was $4.8 million per breach and ranged from $226,000 to $22 million.
- **Direct incremental costs:** averaged $54 per lost record, an 8 percent increase over 2005 results for unbudgeted, out-of-pocket spending. Includes free or discounted services offered; notification letters, phone calls, and emails; legal, audit and accounting fees; call center expenses; public and investor relations; and other costs.
- **Lost productivity costs:** averaged $30 per lost record, an increase of 100 percent over 2005 results, for lost employee or contractor time and productivity diverted from other tasks.
- **Customer opportunity costs:** averaged $98 per lost record, an increase of 31 percent over 2005 results, covering turnover of existing customers and increased difficulty in acquiring new customers. Customer turnover averaged 2 percent and ranged as high as 7 percent.

Other findings:

- **Breach location:** Almost 30 percent of all reported breaches originated with external partners, consultants, outsourcers, or contractors.
- **Breach source:** More than 90 percent of all breaches were in digital form—primarily laptops, electronic backups, and hacked and attacked systems.
- **Groups affected:** Costs were borne primarily by Marketing (55 percent for customer turnover), Customer Support (34 percent for emails, call center, letters), and Legal, Risk Management, and Audit (11 percent for investigations). IT had no direct costs other than to put subsequent preventative measures in place.
- **IT preventative measures:** The cost of new preventative measures averaged 4 percent of the total breach cost, or $180,000 on average. Not all respondents put electronic protections in place.
- **Cost increases:** 75 percent of the increased recovery costs reported between 2005 and 2006 were due to increased expenditures on notification phone calls, offers of free or discounted services, and increased estimates of customer turnover.
- **Response responsibility:** IT executives or IT security were responsible for breach response in 53 percent of incidents. Others responsible included the Business Unit (7 percent), Privacy Officer (7 percent), and Compliance Officer (3 percent). No Single Group (30 percent) was a frequent reply to the question of who was responsible for the breach response.
- **Total cost reported:** The total cost reported by the 31 respondents was $148 million. At $182 per record lost, the total cost of 93 million compromised records reported by the Privacy Rights Clearinghouse is in the billions.

National Consumer Survey on Data Security Breach Notification

In a related survey of 51,000 adult consumers conducted by The Ponemon Institute in 2005, consumers were asked if they had received breach notifications from companies.

- 12 percent of 9,000 respondents had received a notification that their information had been lost
- Extrapolated to the U.S. population, 23 million adults may have received such notifications

Consumers reacted extremely negatively to these notifications and to the companies that mishandled their private and confidential information: almost 60 percent terminated or considered terminating their relationship with the offending company.

Affected individuals created significant damage to corporate reputation, corporate brand, and customer retention:

- Almost 20 percent of respondents terminated their relationship with the company
- A further 40 percent were considering terminating their relationship
- Only 14 percent were “not concerned”

Conclusions

Together, these surveys demonstrate the extreme cost consequence ($182 per record and an average of $4.8 million per incident based on an average of 26,300 records lost) of companies breaching the confidential data and underlying trust of their customers. With the single largest cost being customer turnover, the cost to brand and corporate reputation can be the most long-lasting effect.

In spite of these consequences, new breaches are reported every week. Though security best practices dictate the use of preventative technical solutions, most companies have not yet put such protections in place.

This survey reveals:

- Although effective preventative solutions are deployed by the IT organization, breach recovery costs fall primarily to other corporate groups. Calculating a company-wide risk and ROI for preventative measures cannot be done by IT alone and requires a cross-organizational approach.
- Even after the fact, there are no clear cross-organizational owners for breach recovery. Only 10 percent of companies had a cross-functional topic expert (a Privacy Officer or Compliance Officer) in charge.
- With an average $4.8 million per-incident recovery cost, the ROI calculation on preventative solutions is not too complex. New automated data detection and encryption solutions fall far below this cost threshold.

Preventative Solutions

Automated, cost-effective solutions are now available to secure customer confidential data wherever it is stored or transmitted, both within an organization and among business partners. Centralized deployment of data detection and encryption solutions allows information protection to be aligned with corporate security policies and regulatory mandates. Centralized management allows security best practices to be automatically enforced without relying on individuals to do so and without altering the network environment or email user behavior.

Next Steps

This report allows customers to forecast in detail the specific actions and costs required to recover from a customer data security breach. In turn, they provide a remediation cost profile that can be compared with the technology cost of preventing such an occurrence. This report can be used as a guideline to conduct an internal audit and to create breach notification cost estimates.

Introduction

Stolen laptops, compromised databases, lost backup tapes, or mismanaged email—all can result in the loss of valuable customer information. Organizations that experience a data breach can suffer the loss of existing customer confidence, damage to their brand, and loss of future revenue from new customers that take their business elsewhere. Equally damaging are the actual costs associated with legal requirements to notify customers that their private, sensitive, and confidential information has been mishandled.

As of July 18, 2006, at least 34 states in the U.S. have passed laws[1] requiring organizations and government agencies to notify customers, employees, and other affected individuals when a breach of protected personal information occurs due to human error, technology problems, or malicious acts. Regulations such as California Senate Bill 1386 apply to "any person or business that conducts business in California" even if they are located outside the U.S. In addition, there are currently more than a dozen regulations pending at the federal level in the U.S. Senate and House of Representatives.

Although the specific conditions for notification vary by state, organizations may ***not*** be required to notify individuals when:

- The breached data is protected by at least 128-bit encryption
- The breached data elements are not considered "protected"
- The breach was stopped before information was wrongfully acquired
- Other special circumstances (such as national security or law enforcement investigations) exist

When a breach occurs and customers must be notified, what is the corporate cost to recover? The Ponemon Institute, Vontu, and PGP Corporation are pleased to offer a new survey that quantifies the actual costs incurred by 31 companies compelled to notify customers of data privacy breaches. Summarized in this document, the study provides detailed information from responses to questions companies face when responding to a data breach:

- What are the costs of obtaining legal counsel?
- What are the costs to mail notification letters, call individual customers, recover increased call center costs, or offer discounted products to affected customers in the hope of retaining their business?
- What are the costs of lost customers and brand damage?

[1] State PIRG, "Summary of Security Breach Notification Laws": http://www.pirg.org/consumer/credit/statelaws.htm

Study Overview

The Ponemon Institute's annual benchmark study, begun in 2005, examines the costs organizations incur when responding to data breach incidents resulting in the loss or theft of protected personal information.

- To complete the study, benchmark surveys were sent to companies known to have experienced a breach involving the loss or theft of personal customer, consumer, or student data over the past year.
- Of that group, 31 companies agreed to participate by completing the survey. Results were not hypothetical responses to possible situations; they represent cost estimates for activities resulting from an actual data loss incident.
- Reported number of individual records breached ranged from 263,000 to 815,000 from companies in 15 different industry sectors.
- Survey shows that almost 30 percent of all data breaches are from external sources, including outsourcers, consultants, business partners, and contractors.

Table 1 summarizes the 14 study participants by industry and source of data breach:

Industry	Number	Internal Breach	External Breach
Retail & Online Commerce	7	7	0
Financial Services	5	4	1
Hardware & Software	3	1	2
Services & Outsourcers	3	2	1
Health Care & Benefits	2	1	1
Pharmaceuticals	2	2	0
Insurance	1	0	1
Hotels	1	0	1
Airline	1	1	0
Education	1	1	0
Telecom	1	0	1
Utility	1	1	0
Automotive	1	1	0
Not Disclosed	2	1	1
Total	**31** **100%**	**22** **71%**	**9** **29%**

Table 1: Study Participants & Data Breach Source

Study Methodology

The study looked at core process-related activities associated with a company's detection of and response to a data breach, identifying four "cost centers":

- **Discovery & escalation:** Activities enabling the company to detect the breach of protected data and to report a breach of protected information within a specified time period.
- **Customer notification:** Activities enabling the company to notify affected individuals via letter, telephone, email, or general notice that protected information was breached.
- **Post-notification response:** Activities to help affected individuals communicate with the company to minimize potential damage as well as the cost of credit report monitoring or issuing a new account/credit card.
- **Customer costs:** Costs resulting from the loss of trust by existing customers and customer turnover using the "lifetime value" of an average customer as defined for each participating organization.

The survey asked participants to divide costs among three types:

- **Direct incremental costs:** Estimate of direct expenses to accomplish specific activities
- **Indirect productivity costs:** Estimate of time, effort, and other organizational productivity
- **Customer opportunity costs:** Estimate of lost customers and brand damage

Key Report Findings

Overall costs to recover from a data breach increased 30 percent between the 2005 and 2006 surveys. The average number of records lost declined, but the cost per record increased significantly. Figure 1 on page 8 summarizes report findings.

- **Total per-incident costs** including average direct, indirect, and opportunity costs:
  - o $182 per record or $4.8 million per company
  - o Company costs reported ranged from $226,000 to $22 million
  - o Total of $148 million in costs across the sample of 31 companies
- **Direct incremental costs** for incremental, out-of-pocket, unbudgeted spending for outside legal counsel, mail notification letters, calls to individual customers, increased call center costs, and discounted product offers
  - o $54 per record or $1.4 million per company
  - o An increase of 8 percent over 2005 results

- **Indirect productivity costs** for lost employee productivity
  - $30 per record or $800,000 per company
  - An increase of 100 percent over 2005 results
- **Customer opportunity costs** covering brand damage, loss of existing customers, and increased difficulty in recruiting new customers
  - $98 per record or $2.6 million per company
  - An increase of 31 percent over 2005 results

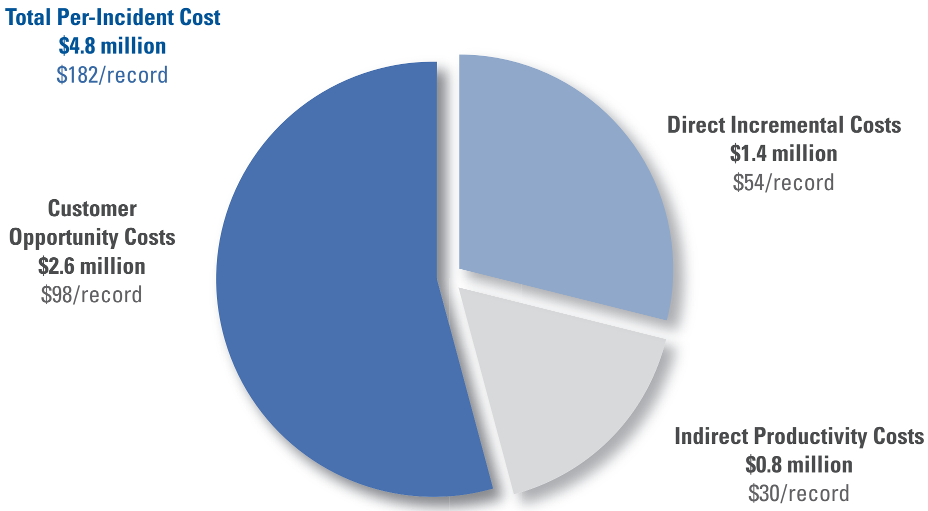


Figure 1: Recovery Cost Averages

Direct incremental costs: largest direct costs were to cover the following activities:

• Free or discounted services	$24 per record
• Notification letters, phone calls, emails, web, media	$13
• Legal defense services & criminal investigations	$ 7
• Legal, audit, and accounting fees	$ 4
• Call center expenses	$ 3
• Public and investor relations	$ 1
• Internal investigations	$ 1

Customer opportunity costs, expressed as the loss of current or potential customers, was the largest single category, as described in Figure 2.

- Average breach was 26,300 customer records
- Average opportunity cost was 2 percent loss of all customers
- Customer loss ranged from 0 to 7 percent, depending on the industry sector
- Averaged $2.6 million per company with breached data
- Averaged $98 per customer whose data was lost

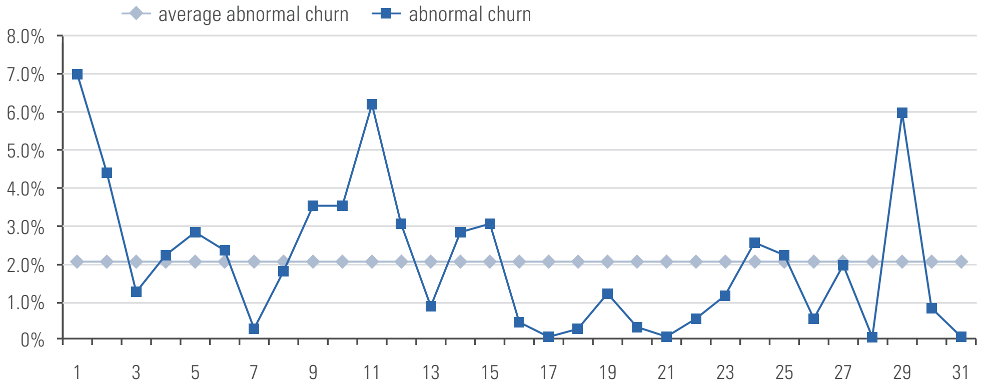


Figure 2: Customer Turnover Variation

Survey of consumers: In a related survey of 51,000 adult consumers conducted by The Ponemon Institute in 2005 ("National Consumer Survey on Data Security Breach Notification"), consumers were asked if they had received breach notifications, as shown in Figure 3.

- 12 percent of the 9,000 respondents had received notification that their data had been lost.
- Extrapolated to the U.S. population, 23 million adults have received such notifications.
- Consumers reacted extremely negatively to notifications and to the companies that mishandled their private and confidential information.
- Almost 60 percent terminated or considered terminating their relationships with offending companies.

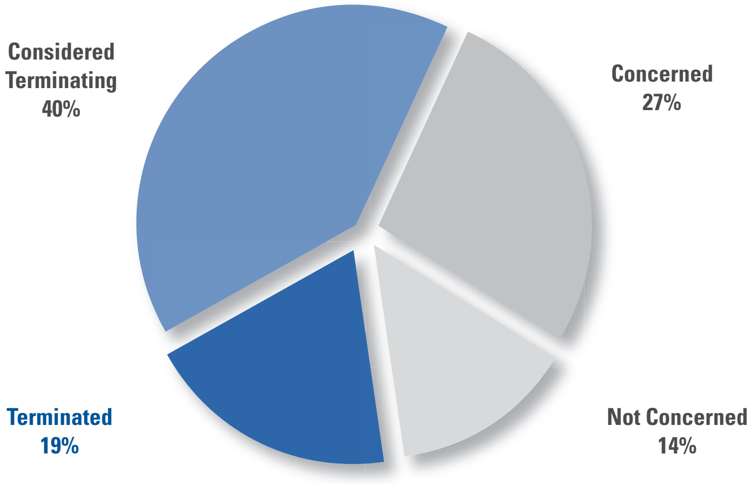


Figure 3: Customer Turnover Impact

Cost by cost center: Among the four major cost centers (discovery & escalation, customer notification, post-notification response, and customer costs), initial costs were lower than downstream post-notification and customer costs, as described in Figure 4.

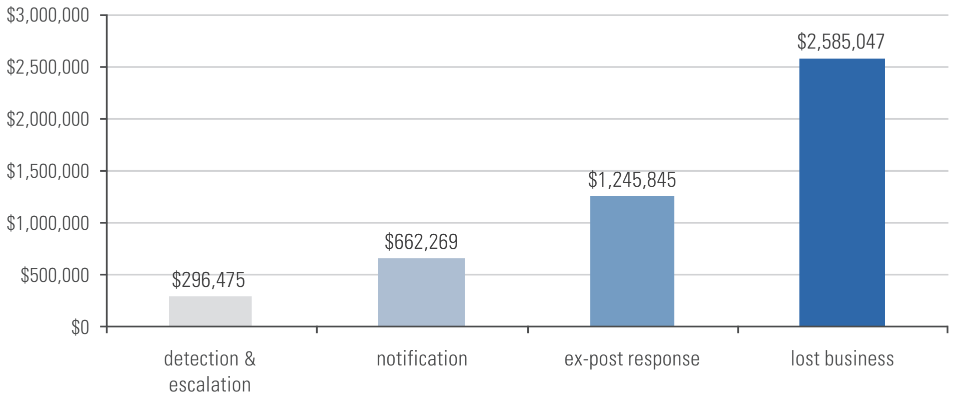


Figure 4: Average Per-Company Cost, by Cost Center

Cost center increase 2005 to 2006: On a per-record basis, all these costs increased from the 2005 survey, as shown in Figure 5.

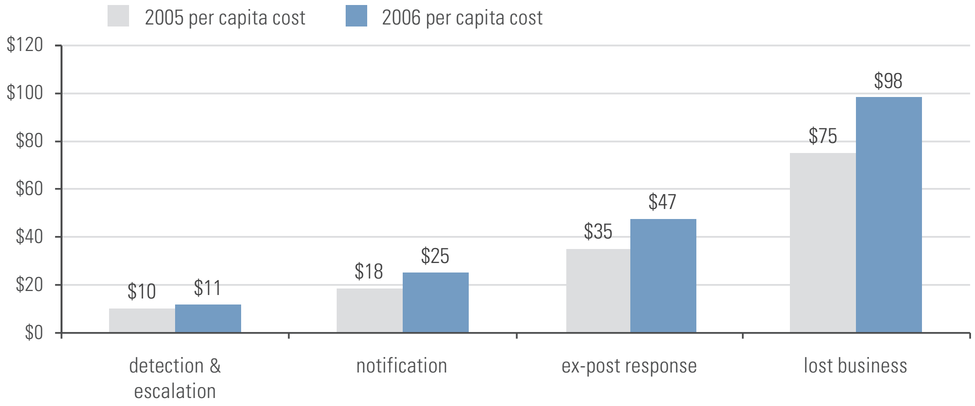


Figure 5: Average Per-Company Cost, by Cost Center

Breach source: The source of more than 90 percent of all breaches was the loss of information in digital form—primarily laptops, electronic backups, and hacked and attacked systems, as shown in Figure 6.

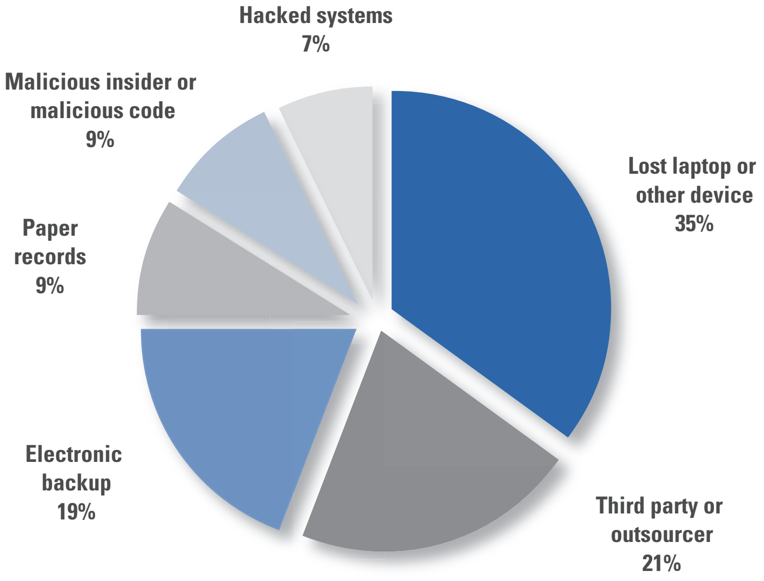


Figure 6: Source of Data Breach

Costs by organization: Costs were borne primarily by Marketing (customer turnover), Customer Support (emails, call center, letters), and Legal, Risk Management, and Audit (investigations), as shown in Figure 7. IT had no direct costs other than subsequent preventative measures, which cost an average of 4 percent of the total breach cost, or $180,000 on average. Not all respondents put electronic protections in place.

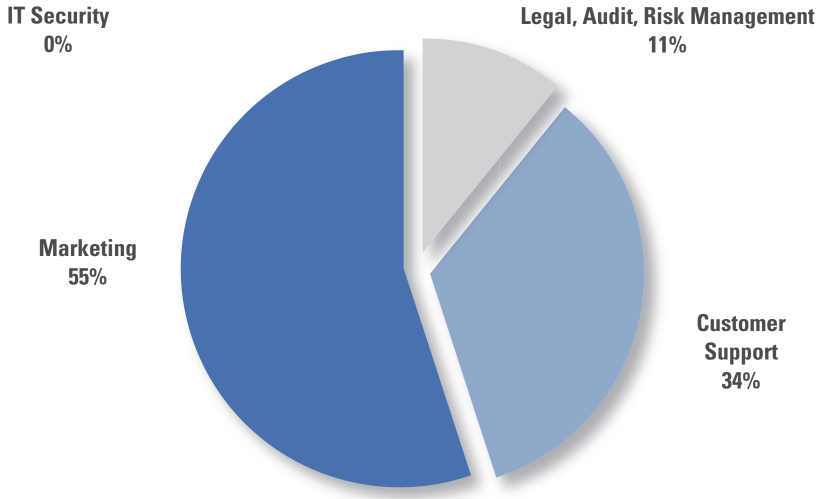


Figure 7: Breach Recovery Cost by Corporate Organization

Response responsibility: IT executives or IT security were responsible for breach response in 53 percent of incidents. Others responsible included the Business Unit (7 percent), Privacy Officer (7 percent), and Compliance Officer (3 percent). No Single Group (30 percent) was a frequent reply to the question of who was responsible for the breach response, as shown in Figure 8.

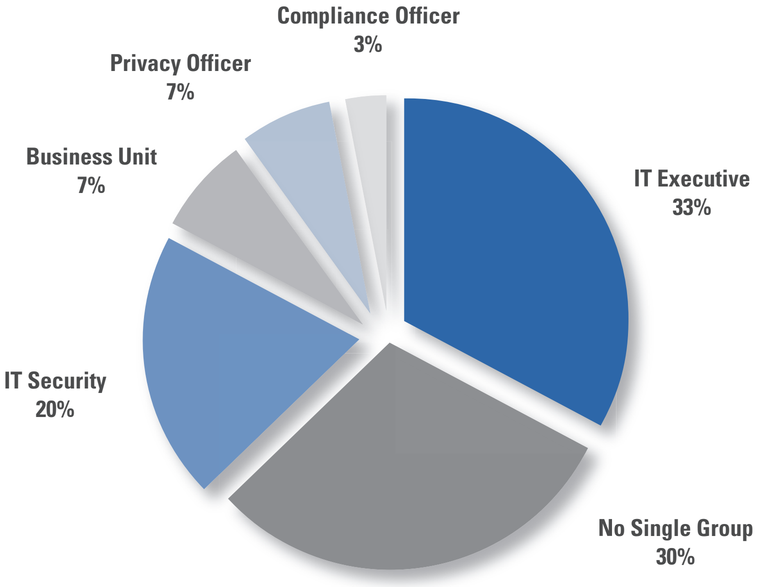


Figure 8: Groups Responsible for Breach Response

Data Breach Costs By Category

Table 2 summarizes results for the average company in the survey by core activity and cost category, **per record lost**.

Cost of Breach Recovery	Direct Incremental Cost	Lost Productivity Cost	Customer Opportunity Cost	Total
Detection & Escalation				
Internal investigation	$ 1.38	$ 4.10	-	$ 5.48
Legal, audit, & consulting	4.38	1.41	-	5.80
	$ 5.76	$ 5.51	-	$ 11.28
Initial Notification				
Letters	$ 5.30	$ 1.11	-	$ 6.41
Emails	0.34	0.53	-	0.86
Telephone	7.30	10.47	-	17.76
Published media	0.03	-	-	0.03
Website	0.06	0.06	-	0.12
	$ 13.03	$ 12.16	-	$ 25.19
Post-Notification				
Mail	$ 0.13	$ 0.10	-	$ 0.23
Emails	0.15	0.86	-	1.00
Telephone to internal call center	1.88	3.28	-	5.16
Telephone to outsourced call center	1.40	4.62	-	6.03
Legal defense services	5.51	1.12	-	6.63
Criminal investigations (forensics)	1.38	1.10	-	2.48
Public or investor relations	1.16	0.89	-	2.05
Free or discounted services	23.80	-	-	23.80
	$ 35.42	$ 11.97	-	$ 47.39
Brand Impact				
Cost of turnover	-	-	$ 93.62	$ 93.62
Cost of fewer new customers	-	-	4.70	4.70
	-	-	$ 98.32	$ 98.32
Total cost of data breach	**$ 54.22**	**$ 127.96**	**$ 98.32**	**$ 182.17**
Post-Event IT Spending	$ 6.85	-	-	$ 6.85

Table 2: Average Per-Record Recovery Costs

Table 3 summarizes results for the **average** company in the survey by core activity and cost category.

Cost of Breach Recovery	Group Affected	Direct Incremental Cost	Lost Productivity Cost	Customer Opportunity Cost	Total
Detection & Escalation					
Internal investigation	Legal	$ 36,313	$ 107,742	-	$ 144,055
Legal, audit, & consulting	Legal	115,227	37,194	-	152,420
		$ 151,540	$ 144,935	-	$ 296,475
Initial Notification					
Letters	Support	$ 139,414	$ 29,077	-	$ 168,491
Emails	Support	8,858	13,873	-	22,731
Telephone	Support	191,814	275,188	-	467,002
Published media	Marketing	919	-	-	919
Website	Marketing	1,674	1,452	-	3,126
		$ 342,680	$ 319,589	-	$ 662,269
Post-Notification					
Mail	Support	$ 3,540	$ 2,500	-	$ 6,040
Emails	Support	3,832	22,500	-	26,332
Telephone to internal call center	Support	49,364	86,275	-	135,639
Telephone to outsourced call center	Support	36,899	121,575	-	158,474
Legal defense services	Legal	144,900	29,516	-	174,416
Criminal investigations (forensics)	Legal	36,377	28,871	-	65,248
Public or investor relations	Marketing	30,482	23,419	-	53,902
Free or discounted services	Support	625,793	-	-	625,793
		$ 931,189	$ 314,656	-	$ 1,245,845
Brand Impact					
Cost of turnover	Marketing	-	-	$ 2,461,401	$ 2,461,401
Cost of fewer new customers	Marketing	-	-	123,646	123,646
		-	-	$ 2,585,047	$ 2,585,047
Total cost of data breach		**$ 1,425,408**	**$ 3,364,229**	**$ 2,585,048**	**$ 4,789,637**
Per-record cost of data breach		$ 54	$ 128	$ 98	$ 182
Post-Event IT Spending	IT Security	$ 180,000	-	-	$ 180,000

Table 3: Average Per-Company Recovery Costs

Table 4 summarizes total results for **all companies** in the survey by core activity and cost category.

Cost of Breach Recovery	Group Affected	Direct Incremental Cost	Lost Productivity Cost	Customer Opportunity Cost	Total
Detection & Escalation					
Internal investigation	Legal	$ 1,125,700	$ 3,340,000	-	$ 4,465,700
Legal, audit, & consulting	Legal	3,572,030	1,153,000	-	4,725,030
		$ 4,697,730	$ 4,493,000	-	$ 9,190,730
Initial Notification					
Letters	Support	$ 4,321,834	$ 901,400	-	$ 5,223,234
Emails	Support	274,606	430,050	-	704,656
Telephone	Support	5,946,238	8,530,820	-	14,477,058
Published media	Marketing	28,500	-	-	28,500
Website	Marketing	51,900	45,000	-	96,900
		$ 10,623,077	$ 9,907,270	-	$ 20,530,347
Post-Notification					
Mail	Support	$ 109,750	$ 77,500	-	$ 187,250
Emails	Support	118,800	697,500	-	816,300
Telephone to internal call center	Support	1,530,298	2,674,519	-	4,204,817
Telephone to outsourced call center	Support	1,143,880	3,768,828	-	4,912,708
Legal defense services	Legal	4,491,900	915,000	-	5,406,900
Criminal investigations (forensics)	Legal	1,127,700	895,000	-	2,022,700
Public or investor relations	Marketing	944,950	726,000	-	1,670,950
Free or discounted services	Support	19,399,570	-	-	19,399,570
		$ 28,866,848	$ 9,754,347	-	$ 38,621,195
Brand Impact					
Cost of turnover	Marketing	-	-	$ 76,303,443	$ 76,303,443
Cost of fewer new customers	Marketing	-	-	3,833,030	3,833,030
		-	-	$ 80,136,472	$ 80,136,472
Total cost of data breach		**$ 44,187,655**	**$ 104,291,089**	**$ 80,136,473**	**$ 148,478,744**
Per-record cost of data breach		$ 54	$ 128	$ 98	$ 182
Post-Event IT Spending	IT Security	$ 5,580,000	-	-	$ 5,580,000

Table 4: Total Recovery Costs, 31 Companies

Report Conclusions

Together, these surveys demonstrate the extreme cost consequence of companies breaching the confidential data and underlying trust of their customers. With the single largest cost being customer turnover, the cost to brand and corporate reputation can be the most long-lasting effect.

In spite of these consequences, new breaches are reported every week. Although security best practices dictate the use of preventative technical solutions, most companies have not yet put such protections in place.

This survey reveals:

- Although effective preventative solutions are deployed by the IT organization, breach recovery costs fall primarily to other corporate groups. Calculating a company-wide risk and ROI for preventative measures cannot be done by IT alone and requires a cross-organizational approach.
- Even after the fact, there are no clear cross-organizational owners for breach recovery. Only 10 percent of companies had a cross-functional topic expert (a Privacy Officer or Compliance Officer) in charge.
- With an average $4.8 million per-incident recovery cost, the ROI calculation on preventative solutions is not too complex. New automated data detection and encryption solutions fall far below this cost threshold.

Preventative Solutions

Automated, cost-effective solutions are now available to secure customer confidential data wherever it is stored or transmitted, both within an organization and among business partners. Centralized deployment of data detection and encryption solutions allows information protection to be aligned with corporate security policies and regulatory mandates. Centralized management allows security best practices to be automatically enforced without relying on individuals to do so and without altering the network environment or email user behavior.

Next Steps

This report allows customers to forecast in detail the specific actions and costs required to recover from a customer data security breach. In turn, they provide a remediation cost profile that can be compared with the technology cost of preventing such an occurrence. This report can be used as a guideline to conduct an internal audit and to create breach notification cost estimates.

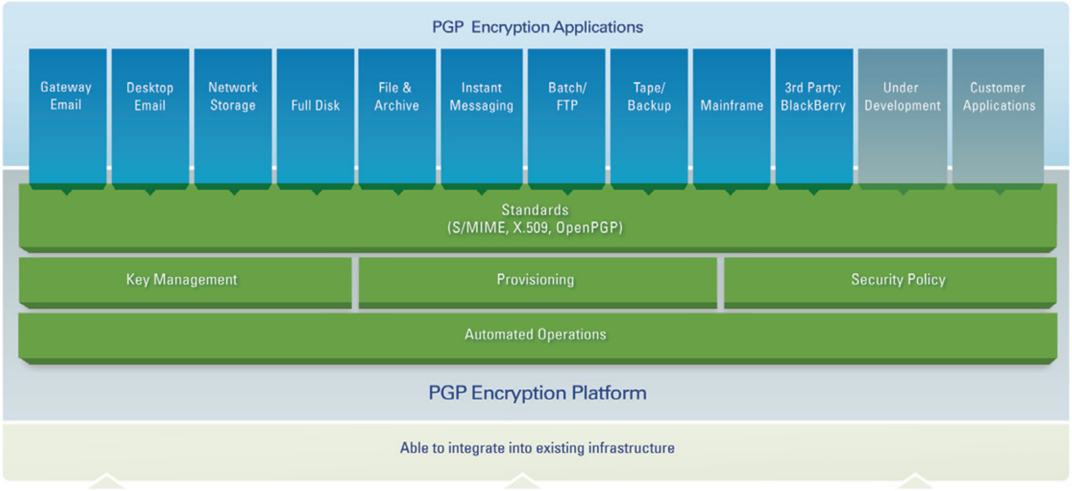
Note: This Report Conclusions section is duplicated at the beginning of the report in the Executive Summary.

PGP Solutions

PGP Corporation has developed the PGP® Encryption Platform to protect confidential information from data breaches, regulatory notification requirements, and resulting remediation costs. This unified platform allows IT organizations a simple, cost-effective way to provide data security to all internal departments and external partners that handle confidential information.

The PGP Encryption Platform allows for central management with automatic operation, email infrastructure transparency, and removal of laptop/desktop, gateway/server, and mobile/wireless encryption silos. It meets business unit requirements for customer privacy, competitive protection, supply chain integrity, and "brand insurance" against public breaches—without disrupting users.

Once deployed, the PGP Encryption Platform is capable of provisioning encryption applications in a combination of gateway and end-point locations. This "deploy-once, enable-over-time" approach allows enterprises to address their greatest risks today and grow into a comprehensive security solution over time.



Current PGP encryption applications:

- **PGP® Whole Disk Encryption:** encrypted full disk, files, folders, USB, & external backups
- **PGP® NetShare:** encrypted files and folders stored on network file servers
- **PGP Universal™ Gateway Email:** gateway encryption & digital signatures
- **PGP® Desktop Email:** desktop encryption, digital signatures, file shred, & IM encryption
- **PGP® Support Package for BlackBerry®:** PGP encryption on BlackBerry handheld devices
- **PGP® Command Line:** encryption for batch processes & FTP transfers
- **PGP® Software Development Kit:** encryption for customized, internal applications

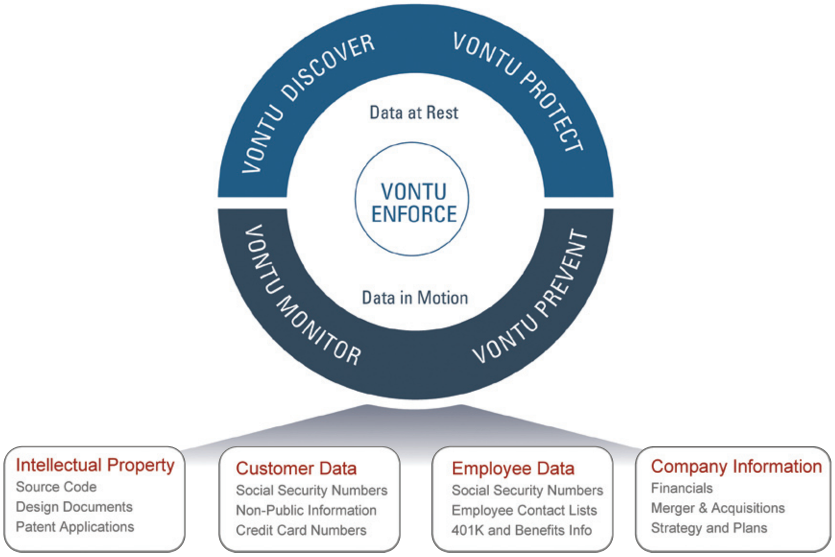
The PGP Encryption platform is an automated, server-based architecture that centrally handles all key management, corporate encryption policy, and network infrastructure interaction. It manages both gateway and client encryption applications, providing one uniform encryption policy that is automatically enforced for all users. Automatic encryption and decryption means no user training, minimal IT resource impact, and low operational costs. Its proxy-based design installs without disruption to existing network architectures and easily expands to meet future risks to data security.

PGP Corporation sets the standard for verifying that no backdoors or secret access exists in its product software. The company is the only commercial security vendor to publish source code for peer review. PGP source code has been downloaded more than 66,000 times. PGP Universal was named Best Encryption Solution (*SC Magazine* Global Awards) and Best Security Solution for Healthcare (*SC Magazine* European Excellence Awards) and was a finalist for Product of the Year (Information Management Awards). PGP Corporation was one of six finalists in *SC Magazine* Global Award's Best Security Company category.

Vontu Solutions

Vontu helps organizations discover and protect confidential data at rest, monitor and prevent data in motion from wrongful disclosure, and automatically enforce data security and privacy policies. With Vontu, organizations reduce the frequency and severity of both inadvertent and malicious data loss incidents to protect brand and reputation, safeguard customer data, protect intellectual property, demonstrate compliance, and reduce the impact of laptop and server theft.

Unified Protection of Data at Rest and Data in Motion



Vontu meets the requirements of global companies and government organizations to:

- Discover and protect confidential data at rest
- Monitor and prevent confidential data in motion
- Accurate detection across all content and groups
- Automate enforcement and response workflow
- Encryption visibility and control
- Safeguard employee privacy
- Proven global scale and architecture

Vontu products include:

- **Vontu Discover:** Detect confidential data at rest on shared file servers, web servers, desktops and laptops.
- **Vontu Protect:** Quarantine or remove exposed confidential data at rest.
- **Vontu Monitor:** Accurately detect all confidential information over all network protocols including encrypted web traffic (HTTPS).
- **Vontu Prevent:** Stop confidential data loss via email, FTP, HTTP or secure HTTP.
- **Vontu Enforce:** Automatically enforce data security policies with centralized management, remediation and compliance reporting.

About The Ponemon Institute

The Ponemon Institute© is dedicated to advancing ethical information and privacy management practices in business and government. 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.

Dr. Larry Ponemon is the chairman and founder of the Ponemon Institute. He is also a founding member of the Unisys Security Leadership Institute and an Adjunct Professor of Ethics & Privacy at Carnegie Mellon University's CIO Institute. Dr. Ponemon is a critically acclaimed author, lecturer, spokesman, and pioneer in the development of privacy auditing, privacy risk management, and the ethical information management process.

Previously, Dr. Ponemon was the CEO of the Privacy Council and the Global Managing Partner for Compliance Risk Management at PricewaterhouseCoopers (where he founded the privacy practice). Prior to joining PricewaterhouseCoopers, Dr. Ponemon served as the National Director of Business Ethics Services for KPMG and as the Executive Director of the KPMG Business Ethics Institute. Dr. Ponemon holds a Ph.D. from Union College, attended the Doctoral Program in System Sciences at

Carnegie-Mellon University, and has a Masters degree from Harvard University as well as a Bachelors degree from the University of Arizona. Contact The Ponemon Institute at www.ponemon.org or
+1 800 887 3118.

About PGP Corporation

PGP Corporation, a global security software company, is the leader in email and data encryption. Based on a unified key management and policy infrastructure, the PGP® Encryption Platform offers the broadest set of integrated applications for enterprise data security. The platform enables organizations to meet current needs and expand as security requirements evolve for email, laptops, desktops, instant messaging, PDAs, network storage, FTP and bulk data transfers, and backups.

PGP solutions are used by more than 30,000 enterprises, businesses, and governments worldwide, including 94 percent of the Fortune® 100 and 76 percent of Germany's DAX Index. As a result, PGP Corporation has earned a global reputation for innovative, standards-based, and trusted solutions. PGP solutions help protect confidential information, secure customer data, achieve regulatory and audit compliance, and safeguard companies' brands and reputations. Contact PGP Corporation at http://www.pgp.com/ or +1 650 319 9000.

About Vontu, Inc.

Vontu is the leading provider of Data Loss Prevention solutions for both data at rest and data in motion. Vontu allows organizations to discover and protect exposed confidential information, monitor all network traffic, block select email, FTP and web communications, and automatically enforce data loss prevention policies. By reducing the frequency and severity of both inadvertent and malicious data loss incidents, Vontu helps organizations ensure public confidence, reduce compliance risk and protect competitive advantage. Vontu customers include Fortune 500 companies in financial services, insurance, high technology, retail, telecommunications, manufacturing, media, and healthcare, as well as state and federal government agencies. Vontu has received numerous awards, including *SC Magazine*'s 2006 U.S. Excellence Award for "Best Enterprise Security Solution" and Global Award for "Best New Security Solution," as well as IDG's *InfoWorld* 2006 Technology of the Year Award for "Best Insider Threat Defense." For more information, please visit www.vontu.com.

Appendix A – Survey Methodology

The Ponemon Institute's study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

- **Non-statistical results:** The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of organizations, all U.S.–based entities experiencing a breach involving the loss or theft of customer, consumer or employee data over the past 12 months. Statistical inferences, margins of error, and confidence intervals cannot be applied to this data given the nature of the sampling plan.

- **Non-response:** The current findings are based on a small representative sample of completed surveys. An initial emailing of benchmark surveys was sent to a reference group of 56 separate organizations, all known to have experienced a breach involving the lost or theft of personal data sometime over the past 12 months. Thirty-one companies completed all parts of the benchmark survey. Non-response bias was not tested, so it is always possible companies that did not participate are substantially different from those that completed the survey in terms of the methods used to manage the data breach process as well as the underlying costs involved.

- **Sampling-frame bias:** Because the sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. The Institute believes that the current sampling frame is biased toward companies with more mature privacy or information security programs.

- **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, The Institute decided to omit other important variables such as leading trends and organizational characteristics from its analyses. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.

- **Estimated cost results:** The quality of survey research is based on the integrity of confidential responses received from companies. Although certain checks and balances can be incorporated into the survey process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique (termed "shadow costing method" explained later) rather than actual cost data could create significant bias in presented results.

Benchmark Methods

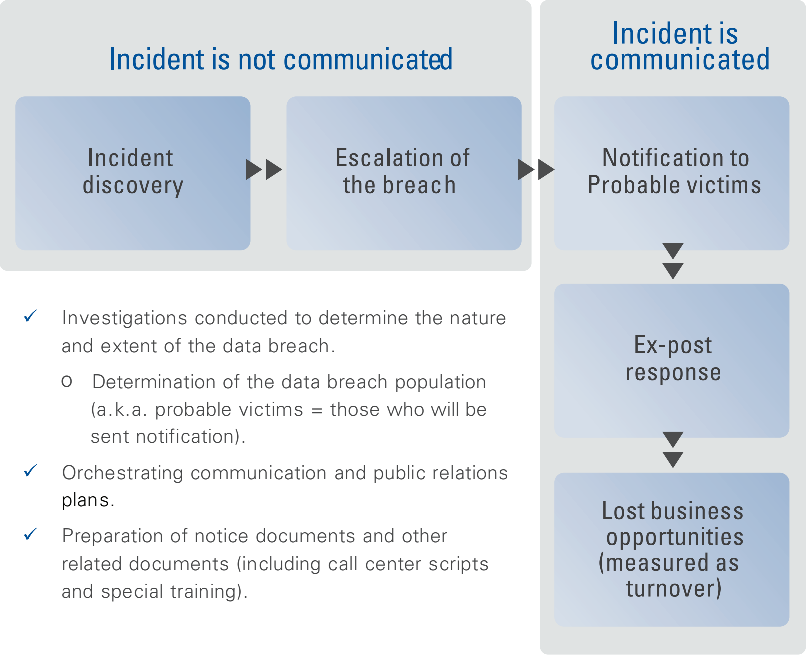
The benchmark survey instrument was designed to collect descriptive information from data protection or information security practitioners about the costs incurred either directly or indirectly concerning the breach event. It also required practitioners to estimate the opportunity cost associated with different program activities. Data was collected on a survey form. The researcher conducted a follow-up interview to obtain additional facts, including estimated abnormal customer turnover rates that resulted from the breach event.

The survey design relied upon a shadow costing method used in applied economic research. This method does not require subjects to provide actual accounting results, but instead relies on broad estimates based on the experience of the subject.

Within each category, cost estimation was a two-stage process. First, the survey required individuals to provide direct cost estimates for each privacy cost category by checking a range variable. A range variable was used rather than a point estimate to preserve confidentiality (to ensure a higher response rate). Second, the survey required participants to provide a second estimate for both indirect costs and opportunity costs, separately. These estimates were calculated based on the relative magnitude of these costs in comparison to direct costs within a given category.

The size and scope of survey items was limited to known cost categories that cut across different industry sectors. The Institute believed that a survey focusing on process (and not areas of compliance) would yield a higher response rate and better quality of results. It also used a paper instrument, rather than an electronic survey, to provide greater assurances of confidentiality.

The diagram below illustrates the activity-based costing schema used in the current benchmark study. The study examined the above-mentioned cost centers. The arrows suggest that these cost centers are sequentially aligned, starting with incident discovery and proceeding to escalation, notification, ex-post response, and culminating in lost business. The cost driver of ex-post response and lost business opportunities is the public disclosure or notice of the event.


Incident is not communicated
Incident is communicated
Incident discovery
Escalation of the breach
Notification to Probable victims
Ex-post response
Lost business opportunities (measured as turnover)

- ✓ Investigations conducted to determine the nature and extent of the data breach.
  - o Determination of the data breach population (a.k.a. probable victims = those who will be sent notification).
- ✓ Orchestrating communication and public relations plans.
- ✓ Preparation of notice documents and other related documents (including call center scripts and special training).

Figure 9: Visual Representation of Benchmark Cost Categories