

The Privacy Management Toolkit

A complete set of privacy management tools

Version 1.0

Rebecca Herold, CISSP, CISM, CISA, FLMI



InformationShield

Information Shield Publishing
Houston, Texas



The Privacy Management Toolkit

By Rebecca Herold, CISA, CISSP, CISM

© 2005 Information Shield, Inc. All rights reserved.

Printed in the United States of America.

Published by Information Shield, Inc., 2660 Bering Dr., Houston, TX 77057.

Contributing Editor: David J. Lineman
Graphic Design: Kristi Sadler, FreshID

The right to use the material found in this guide and related storage media (CD-ROM, floppy disks, etc.) is granted only to licensed and registered purchasers. This guide is sold on an individual copy basis. An organization-specific license to copy, modify, and republish parts of this guide as in-house documentation is granted only to registered purchasers for internal use only. This material is for internal use only at licensee organizations, and may not be remarketed or redistributed. Consultants, VARs, OEMs, and other third parties using this material on behalf of another organization must purchase separate licenses for each organization where this material is used.

No part of this material may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without the written permission of the copyright owner, except where permitted by law.

The information in this reference guide and accompanying storage media is provided as a service to the business community. At the time of its preparation, the policies and other materials found in this guide are believed to be current, relevant, useful, and appropriate for organizations concerned about information security. Such information is nonetheless subject to change without notice. Although every reasonable effort has been made to ensure the accuracy, completeness, and relevance of the information contained herein, the author and the publisher (Information Shield, Inc.), including their affiliates, cannot be responsible for any errors and omissions, or any party's interpretations or applications of the ideas or words contained therein.

Please note: This Toolkit does not represent legal counsel or legal interpretation. It is provided as a guide to help information security, privacy and compliance professionals identify the many types of personal information that may be considered as personally identifiable information within multiple laws. Readers preparing policies and related materials based on this publication are strongly encouraged to seek the advice and guidance of legal counsel trained in information technology and data privacy issues. Neither the author nor Information Shield Inc., nor any of their affiliates, make any warranties, guarantees, or representations about the fitness for any purpose of the information security policies and related material found in this guide.

Purchasers are encouraged to register their license at www.informationshield.com.

ISBN # 1-881585-10-7

Library of Congress Control Number: 2005934796

Also published by Information Shield:

Information Security Policies Made Easy, by Charles Cresson Wood, CISSP, CISM, CISA

Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood, CISSP, CISM, CISA

Employee Information Security Made Easy, by David J. Lineman

Dedication

To my beautiful sons, Heath Xavier and Noah Theodore.



Table of Contents

Chapter 1: Privacy Impact on Business.....	1
The Current State of Privacy Concerns	1
Privacy Incidents Are Increasing	2
Privacy is a Core Business Issue.....	3
Increasing Privacy and Security Threats and Breaches	4
Privacy Related Laws Impact Business	6
The Financial Impact of Privacy on Business.....	7
Why You Might Be At Risk	11
What this guide can do for you	11
Using this guide	14
Using the Sample Policies and Forms	17
Balancing Trade-Offs.....	17
Need For Competent Advice	18
Chapter 2: Creating a Privacy Governance Program.....	19
Defining Privacy Governance.....	19
Why is a Privacy Governance Program Necessary?.....	19
You Must Know What to Protect.....	20
Protect Your Business; Avoid Privacy Mistakes	21
Building Your Privacy Governance Program.....	23
Know Your Business	23
Perform a Privacy Impact Assessment (PIA)	24
Develop Your Privacy Governance Program	25
Establish Privacy Leadership.....	26
The Privacy Official.....	26
The Privacy Team.....	27
Protect Privacy within Customer Relationship Management	28
Secondary Use of Data.....	29
Data Mining Threats to Privacy.....	30
Establish Privacy Policies and Procedures	30
Web Site Privacy Policy	31

Organizational Privacy Policies.....	33
Educate all personnel and business partners on privacy requirements	33
Document Your Privacy Education Program	35
Develop a Privacy Education Strategy	35
Keep the Privacy Education Program Current.....	38
Establish controls to support privacy policies	39
Integrate Privacy into Systems Development.....	40
Use Privacy Enhancing Technologies (PETs)	41
Monitor Security and Privacy Related Laws	42
Define and document the PII your organization handles and map the data flows.....	43
Establish privacy incident response procedures	45
Create a sanctions policy for non-compliance with privacy policies	46
Determine Incident Financial Impact.....	46
Communicate Leading Practices to Executives	47
Summary	48
Chapter 3: Defining Personally Identifiable Information.....	49
What is Personally Identifiable Information?.....	49
Personal Information in the News.....	49
How Does the Definition Vary Across the Globe?.....	50
Regulatory and Legal Definitions.....	51
What Do YOU Consider As Personally Identifiable Information?	57
Summary of Steps to Identify PII within an Organization	58
Chapter 4: OECD Privacy Principles	59
OECD Background and Privacy Principles.....	59
The OECD Privacy Principles	60
Using this guide for OECD compliance	61
World-wide Laws Constructed Around the OECD Principles	62
Standard Contractual Requirements	62
Privacy Principle 1: Collection Limitation Principle.....	66
Privacy Principle 2: Data Quality	70
Privacy Principle 3: Purpose Specification Principle	73
Privacy Principle 4: Limiting Use, Disclosure and Retention Principle.....	78
Privacy Principle 5: Security Safeguards Principle	83

Privacy Principle 6: Openness Principle.....	89
Privacy Principle 7: Individual Participation Principle	92
Privacy Principle 8: Accountability Principle.....	95
Privacy Principle 9: Free Flow of Personal Information and Restrictions	99
Chapter 5: U.S. Privacy Related Laws.....	102
How to Use This Chapter.....	102
Background Discussion	102
Specific Laws to Consider	103
1) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)	103
2) Children’s Internet Protection Act of 2001 (CIPA).....	105
3) Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)	106
4) Fair Credit Reporting Act of 1999 (FCRA).....	108
5) Children’s Online Privacy Protection Act of 1998 (COPPA).....	110
6) Health Insurance Portability and Accountability Act of 1996 (HIPAA).....	113
7) Telecommunications Act of 1996.....	117
8) Electronic Freedom of Information Act of 1996 (E-FOIA)	119
9) Family Education Rights and Privacy Act of 1974 (FERPA; also known as the Buckley Amendment)	121
10) Right to Financial Privacy Act of 1978 (RFPA)	123
11) Privacy Protection Act of 1980 (PPA)	125
12) Cable Communications Policy Act of 1984 (Cable Act)	127
13) Electronic Communications Privacy Act of 1986 (ECPA)	128
14) Computer Security Act of 1987.....	130
15) Video Privacy Protection Act of 1988.....	131
16) Telephone Consumer Protection Act of 1991 (TCPA)	133
17) Driver’s Privacy Protection Act of 1994	135
18) Communications Assistance for Law Enforcement Act of 1994 (CALEA)....	137
19) Computer Fraud and Abuse Act of 1986 (CFAA)	139
20) California Senate Bill 1386 (SB 1386).....	140
21) Fair and Accurate Credit Transactions Act (FACTA) of 2003	143
22) Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003	145

Other U.S. Privacy Related Laws	146
Chapter 6: International Privacy Related Laws	147
How to Use This Chapter	147
Background Discussion on International Privacy Laws	147
Specific Laws to Consider	148
1) European Union Data Protection Directive of 1998.....	148
2) Canada: Personal Information Protection and Electronic Data Act (PIPEDA) of 2000 (also known as Bill C-6)	150
3) Japan: Personal Information Protection Law.....	154
4) Australia: Privacy Act of 1988.....	156
5) New Zealand: Privacy Act, May 1993; Privacy Amendment Act, 1994	161
Other International Laws	167
Chapter 7: Privacy Enhancing Technologies	168
How to Use This Chapter	168
Background.....	168
Specific Privacy Enhancing Technologies.....	170
PET 1: Encryption.....	170
PET 2: Steganography	175
PET 3: Platform for Privacy Preferences (P3P).....	177
PET 4: Privacy Seals.....	179
PET 5: Blind signatures	182
PET 6: Biometrics.....	184
PET 7: Pseudonymous and Anonymous systems	189
PET 8: Enterprise Privacy Authorization Language (EPAL)	191
PET 9: Message Filtering.....	192
PET 10: Pop-up Blockers.....	194
PET 11: Cookie Managers and Bug Zappers.....	195
PET 12: Spyware Management	196
Chapter 8: Privacy Inhibiting Technologies.....	198
How to Use This Chapter	198
Background.....	198
Specific Privacy Inhibiting Technologies.....	199
PIT 1: Cookies	199

PIT 2: Web Bugs.....	203
PIT 3: Spam	206
PIT 4: Spyware	210
PIT 5: Systems, Web Server and Applications Logs.....	215
PIT 6: RFID Tags.....	219
PIT 7: Surveillance Systems	224
Appendix A: Privacy Glossary	228
Appendix B: Privacy Resources	242
Government Agencies.....	242
Email lists (listservs).....	244
Membership Organizations.....	245
Books	245
Whitepapers and Research.....	246
Appendix C: Privacy Officer Checklist	247
Appendix D: Sample CPO Job Description.....	248
The Privacy Officer Role	248
Background and Compensation	249
Knowledge and Responsibilities.....	249
Appendix E: Sample Privacy Incident Response Form	253
Appendix F: Privacy Breach Impact Worksheet	256
Appendix G: Privacy Impact Assessment	257
Appendix H: Executive Privacy Presentation	258
Appendix I: Sample External Privacy Policy	260
The Need for a Web Site Privacy Policy	260
Creating a Web Site Privacy Policy.....	260
Sample Policy	261
Instructions for Use.....	261
Appendix J: Sample Privacy Assessment Questionnaire for Employees	270
Appendix K: References	274
About the Author	284
Providing Feedback	286
Index.....	287

Chapter 1: Privacy Impact on Business

The Current State of Privacy Concerns

Addressing privacy concerns, implementing enterprise security and ensuring compliance to applicable privacy laws are significant to achieving uninterrupted business processing, demonstrating due diligence and minimizing risks due to noncompliance. If an organization is unprepared, a privacy or security breach could result in significant business down time and monetary loss. Security and privacy breaches can negatively impact an organization's reputation, generate legal fines and penalties, and possibly result in costly civil suits that negatively impact customer satisfaction and loyalty and result in significant loss of customers.

The following are just a few examples of privacy-impacting events that have recently occurred:

- June 6, 2005: Citigroup Inc. reported that computer tapes containing personal data on 3.9 million loan customers had been lost by United Parcel Service.
- May 22, 2005: CardSystems Solutions became aware that intruders had cracked into their systems and took 40 million account records for holders of MasterCard, Visa USA, American Express and Discover cards. Visa International and MasterCard Australia Ltd. reported June 21, 2005 that this breach affected 130,000 Australian credit card holders and 67,000 Japanese credit card holders.
- April 28, 2005: Police in Hackensack, N.J. announced arrests for a theft ring that illegally posed as a collection agency. Account information on close to 1 million customers of Commerce Bank, PNC Bank of Pittsburgh, Wachovia and Bank of America. Nine were charged, including seven bank employees.
- March 9, 2005: The personal information of 312,000 LexisNexis consumers were reported as being accessed through fraudulent use of legitimate customer identifications and passwords from its Seisint database.
- March 8, 2005: DSW Shoe Warehouse reported hackers stole data. Subsequent investigation revealed the hackers extracted data on 1.4 million credit cards; they also got driver's license and checking account numbers from 96,000 checking transactions.
- February 25, 2005: Bank of America confirmed computer data tapes containing personal and account information for 1.2 million federal government charge card program customers were lost during shipment to a backup data center.
- July 21, 2004: The DOJ charged a Florida man with the theft of 8.2 gigabytes of personal information worth over \$7 million from Acxiom Corp.

- July 16, 2004: The American Management Association (AMA) 2004 annual survey showed a 6% increase in the number of e-mails subpoenaed as part of a lawsuit or regulatory investigation.
- March 16, 2004: Hackers stole thousands of customer credit card numbers from BJ's Wholesale Club.
- In 2002 Canada launched approximately 1,700 investigations for PIPEDA violations.
- During 2001 – 2002 the Hong Kong Privacy Commissioner Office completed 483 privacy complaint cases.

Privacy Incidents Are Increasing

Statistics reveal the trend is for information privacy and security incidents to continue to rise. For example:

- From the [Federal Trade Commission](#): Occurrences of identity theft continue to rise
 - In 2001: 86,212
 - In 2003 & 2004 combined: 10 million

Identity theft is currently the fastest growing information-related crime.

- From [Anti-Phishing Working Group](#) (APWG): The number of phishing attacks is quickly growing
 - November, 2003: 28 reported unique attacks
 - April, 2005: 2,854 reported unique attacks
 - Average monthly increase in phishing attacks from July, 2004 to April, 2005: 15%
- From [CERT/CC 2004 E-Crime Watch Survey](#): The number of cyber-incidents continues to rise
 - 43% of organizations reported an increase in e-crimes and intrusions from 2003
 - 70% of organizations reported at least one e-crime or intrusion was committed

The [Privacy Rights Clearinghouse](#) started keeping track of reported PII breaches within the United States in early 2005. Between February 15, 2005 and December 1, 2005 they had logged 95 breaches reported in the news. These breaches cumulatively involved the PII of 51.8 MILLION people.

Privacy is a Core Business Issue

As awareness of privacy and related issues grows, organizations must treat privacy as a core business issue or find itself at a disadvantage in the marketplace. Customers are increasingly inclined to seek to do business with organizations that can give them control over their personal information. Information privacy is becoming essential to maintain a competitive edge, profitable growth, legal compliance, a trusted commercial image and meeting a standard of due care.

Based on results from a [Ponemon Institute study](#) reported on June 10 of 2004 that polled over 6,300 consumers, the top ten trusted companies for privacy in the U.S. are eBay, American Express, Procter & Gamble, Amazon, Hewlett Packard, U.S. Postal Service, IBM, Earthlink, Citibank and Dell. The study revealed the three top criteria that consumers use to determine a company's trustworthiness include the company's overall reputation for product and service quality, followed by the company's limits on collection of its customers' personal information, and the use of advertisements and solicitations that respect consumer privacy. Yes, two out of three involve privacy! Does your organization meet these privacy criteria?

Businesses, including an organization's competitors, are becoming acutely aware of the trend to address privacy and use privacy assurances as a differentiator for keeping, and obtaining new customers. A clear example of this is Hewlett Packard (HP). In 2003 HP awarded the first [HP Privacy Innovation Award](#) at the PrivacyCon conference to "recognize world-wide leadership in privacy protection and practices." eBay and the Office of the CIO of the Government of Alberta, Canada received the 2003 awards. It is reported that HP plans to make this an annual award.

Another indicator of the trend to promote and implement privacy assurances is the amount of budget organizations are allotting to privacy initiatives. For example, in March 2004, the Ponemon Institute (see [Appendix K](#)) released the results of a different study funded by IBM that revealed that privacy protection is growing in importance for businesses. The study shows that spending on privacy protection increased noticeably the further along organizations were in the privacy initiative implementation process. Spending on privacy initiatives among the forty-four U.S.-based organizations surveyed varied from approximately \$500,000 to about \$22 million annually. This wide range in budget is attributed to the varying stages of privacy implementation of the respondents. The privacy activities being performed within the organizations varied depending upon the stage of privacy program implementation. At a high level the study found:

- According to industry classification, technology companies spend the most on privacy initiatives. Companies in heavily regulated industries, such as financial services and health care, spend within the middle range among other industry groups. Transportation and hospitality companies spend the least on privacy initiatives as compared to other industry groups.

- Early stage privacy implementation companies plan significant increases in spending as their privacy programs enter a more advanced stage.
- Privacy spending increases result from activities such as running employee training sessions, performing self-assessments, conducting independent audits, securing vendor relationships and obtaining Web site privacy assurance certification.
- As company privacy initiatives progress, average spending is expected to increase from \$3.9 million to almost \$14 million, an increase of approximately 355% from early to late stage implementation.
- Ten percent of the companies surveyed are using privacy enabling technologies (such as encryption) that directly enhance compliance and mitigate business risk.

Yet another Ponemon Institute study of 64 companies from 2005 (see [Appendix K](#)) revealed that companies with designated chief privacy officers (CPOs) who have at least a dotted-line relationship to the CIO tend to have the most effective privacy programs.

Increasing Privacy and Security Threats and Breaches

Increasingly, organizations and their information systems and networks are faced with information privacy and security threats from a wide range of sources such as identity theft, mistakes, lack of knowledge, inappropriate business practices, computer-assisted fraud, sabotage, vandalism, and fire or flood. Privacy risks such as e-mail schemes, identity theft, fraud, and so on have become more common, more ambitious and increasingly sophisticated. Additionally, the number of privacy-related laws and regulations continues to proliferate at exponential rates throughout the world.

Dependence on information systems, applications services and personnel knowledge of risk means organizations are more vulnerable to information privacy and security threats. The interconnecting of public and private networks, trends toward distributed computing, connections to business partners and third parties, and sharing of information resources increases the difficulty of achieving adequate and acceptable information protection and access control. The large number of laws requiring privacy and security activities can be overwhelming if there is not one person or business area responsible for knowing, understanding and addressing the requirements. Monitoring the laws is necessary to ensure compliance and to prevent being fined or undergoing legal action as a result of noncompliance. In [Chapter 5](#) and [Chapter 6](#), I list a number of U.S. and international privacy laws that you should monitor.

So, could a privacy breach impact your organization? Organizations have been significantly impacted by privacy incidents they could have prevented with an effective privacy governance program. The following are just a few examples of the privacy incidents and suits that have occurred and impacted businesses recently:

- July, 2005: CardSystems Solutions Inc. is poised to go out of business as a direct consequence of a May 2005 security breach in which 40 million credit card numbers stored on their internal network were accessed by attackers who defeated the perimeter security. The company announced the breach May 22nd, and on July 19th, both Visa and American Express announced that they would no longer use CardSystems Solutions.
- June, 2005: As a result of data theft resulting from criminals posing as a legitimate business, personal information for over 145,000 consumers listed in the ChoicePoint Inc. databases has cost the company, as of June 2005, \$12 million in legal expenses, professional fees, communications to affected consumers. ChoicePoint reports that also as of June 2005 the information stolen has been used in around 750 identity-theft scams. The stock value dropped 24% after the incident was announced.
- July 19, 2004: Scott Richter and his Westminster, Colo., marketing company, OptInRealBig.com agreed to pay New York state \$50,000 in penalties and costs and adhere to certain standards and safeguards in his e-mail practices, under a court settlement announced by New York State Attorney General Eliot Spitzer.
- May 12, 2004: NCO Group, Inc. was ordered to refrain from future violations of the Fair Credit Reporting Act (FCRA) and must pay a \$1.5 million civil penalty to resolve accusations of illegal conduct (filing inaccurate information about consumer accounts to credit bureaus) in violation of the FCRA according to a judgment by the government in the U.S. District Court for the Eastern District of Pennsylvania.
- April 16, 2004: Defendant companies were ordered by the FTC to Pay \$11.8 million for consumer redress, barred from violating the Telemarketing Sales Rule (TSR) as a result of the FTC's "Dialing for Deception" (marketing activity considered as telemarketing fraud) law enforcement sweep.
- February 11, 2004: A Canadian bank was found guilty of PIPEDA violations.
- In November 2003: The FTC filed a lawsuit alleging a variety of deceptive practices by AmeriDebt, Inc., one of the nation's largest credit counseling agencies (CCAs), its former service provider (DebtWorks, Inc.), and DebtWorks' owner, Andris Pukke. At the same time, the Commission entered into a settlement with the Ballenger Group, LLC, AmeriDebt's service provider, for its role in the deception. In related areas, the Commission has brought two lawsuits against debt negotiators, and numerous cases against credit repair organizations. The Commission continues to conduct non-public investigations of additional CCAs, debt negotiators, and related entities.
- November 7, 2003: A Canadian telecommunications company was found guilty of violating federal privacy laws.
- October 31, 2003: A Canadian telecommunications company's collection of its employees' personal health information and its procedures for safeguarding that information was ruled to be in violation of PIPEDA requirements.

- July 30, 2003: The FTC ordered Equifax to pay \$250,000 for FCRA violations charging Equifax did not have sufficient personnel available to answer the toll-free phone number provided on consumers' credit reports.

Privacy Related Laws Impact Business

The number of laws and regulations that govern how personal information must be handled continues to grow worldwide. For example, the [European Union \(EU\) Data Protection](#) law (See [Chapter 6](#), International Privacy Laws) impacts the activities of any office located outside the EU that receives, from an entity in the EU, any information considered as personal information. These restrictions result from the 1995 EU Data Protection Directive that provides detailed requirements regarding the treatment of personal data, and which requires each of the EU Member States to enact national legislation to conform its law to those requirements. Organizations doing business in EU countries must understand and comply with the requirements and laws.

As another example, U.S. [California SB 1386](#), became law on July 1, 2003 and requires all companies that maintain information about California residents in computerized formats to promptly notify through one of four possible ways each of their California customers in the event a security breach occurs that involves improper access to the resident's unencrypted personally identifiable information (PII). SB 1386 authorizes any person injured by a violation of this statute to institute a civil action to recover damages. The statute also authorizes mandates against businesses that violate or propose to violate the statute; so a court may force a business to disclose a breach and possibly discontinue business until evidence is provided the breach has been addressed. In addition to legal and monetary penalties, additional impact resulting from a security breach and SB 1386 noncompliance is negative publicity and lost business. SB 1386 provided the impetus for many U.S. Federal bills and widespread passage of state-level breach laws. In 2005 breach notification legislation was enacted in at least 22 U.S. states by December 10, and was being considered in at least 14 other states.

Organizations have been impacted by SB1386, and have had to use significant human and financial resources to comply with the law following security breaches. For example:

- March, 2004: Texas-based web site hosting company Allegiance Telecom Inc. and two of its subsidiaries sent letters to more than 4,000 customers in the first two weeks of the month to notify them of two computer security breaches that may have involved account or customer information in processing facilities in Boston to comply with SB1386. Although the law requires notification of California customers only, the company sent the letters to customers both within and outside California.
- February 11, 2004: The California Employment Development Department sent letters to approximately 55,000 household employees after a hacker accessed a department server containing workers' private information. It appeared the hacker primarily used

the server to send spam; the extent of the hacker's access to the private information could not be determined.

- December 30, 2003: A laptop computer, owned by United Blood Services and containing personal information on 38,000 California blood donors, was stolen from a repair shop in Scottsdale, Arizona. Notices were mailed February 9, 2004.
- November 15, 2003: Wells Fargo Bank sent letters to over 200,000 customers after a laptop containing confidential information, including names, addresses, Social Security numbers, and personal line of credit account numbers, was stolen. The bank is monitoring the accounts, changed account numbers, and is paying the one-year membership cost of a credit monitoring service for affected customers. In addition to mailing the letters, Wells Fargo also provided a toll-free number to call for additional information and offered a \$100,000 reward for information leading to the thief's arrest. Wells Fargo had notification procedures in place to comply with SB 1386 when the breach occurred.

The Financial Impact of Privacy on Business

A privacy breach could significantly impact your organization's business as it has impacted these businesses. A breach could potentially cost hundreds of thousands to millions of dollars in human resources, communications, and materials expenses in addition to negative publicity, lost business, and legal counsel costs.

As an example, let's examine how it could impact a hypothetical business, Company X. Using data from the U.S. Federal Trade Commission (FTC) on the incidence of and damages from identity theft, almost 5% of persons whose information is stolen or inappropriately accessed will become victims of identity theft and will experience an average damage loss per victim of \$500. If a security breach occurred at a small- to medium-sized Company X for a file containing unencrypted PII for 10,000 customers, at a high level, the following is an example of some of the activities and associated conservatively estimated times in total personnel man-hours that would have a financial and human resource impact to the organization:

Table 1-1: Privacy Incident Business Impact Example

Breach Impact Components	Hours/Cost
Time (in man-hours) to determine and confirm the files within which a breach of PII occurred	40
Time to determine all the individuals impacted	40
Time to collect contact information for impacted customers	60
Time to write and mail letters to notify customers of the breach	60
Time to create and update a web page containing information about the breach	48
Time to answer customer questions about the breach	500
Total Man-Hours	748
Avg. Cost per Man-Hour Cost (include all HR benefit considerations)	\$200.00
Total Man-Hour Costs	\$149,600.00
Estimated cost of materials	
Letter paper and envelopes	1000
Postage (\$0.37 * # of individuals)	3700
Total Materials Cost	\$4,700.00

Now consider the potential that one or more of these customers would bring a civil suit to Company X if they believe they suffered damage as a result of the breach, or if they believe they were not contacted quickly enough following the breach. Using the FTC statistics, 500 customers could be likely victims of identity theft, with an average of \$500 loss per customer this would result in a class action suit claiming \$250,000 in damages, plus the costs for negative publicity and for defending the suit.	
Total number of impacted individuals	10000
Percentage bringing civil suit	5%
Number bringing civil suit	500
Average award to each individual	500
Total cost of award (amount Company X must pay)	\$250,000.00
Fines and penalties for applicable laws	\$250,000.00
Cost to Change/Repair System where Breach Occurred	\$150,000.00
Although not a legal requirement, Company X may choose to pay for impacted customers credit report monitoring since other companies have set a precedent by performing this activity. The costs for ongoing monitoring of credit monitoring vary greatly among the monitoring agencies. However, using a conservative cost of \$100 per customer per year for three years, this could cost around \$1,000,000	

for the 10,000 affected customers.	
Cost per individual for credit reports	1,000,000
Number of years to pay for credit report	3
Total amount for credit reports for all impacted individuals	\$3,000,000.00
Legal costs	\$100,000.00
Stock value before incident	3.5
Stock value after incident	2
Number of shares	2000000
Share value loss	\$3,000,000.00
Number of customers loss	10000
Value per customer	200
Total customer loss	\$2,000,000.00
Total Business Impact of a Privacy Breach	\$10,879,300.00

What impact would a similar incident have upon your organization? Just one incident involving a breach of customer privacy could demonstrably have a significant detrimental financial impact on your business. See [Appendix E](#) for an expanded spreadsheet version

of this privacy incident business impact worksheet with more potential costs to an organization.

Why You Might Be At Risk

Small to medium sized organizations face the same issues as larger enterprises as they progress through the various stages of adopting privacy practices. Unfortunately many of these small and medium businesses are unaware of potential risks or mistakenly believe that, unlike larger businesses, their relative size protects them against risk. In fact, there are very few, if any, companies in the world that are not at risk of being impacted by a privacy incident. Any company is at risk that:

- Has customers or employees
- Has posted a privacy policy
- Has offices located outside the United States
- Is in the healthcare, financial or information handling industry
- Has applicable data protection and privacy laws and regulations
- Handles PII for other organizations

It is incumbent upon every organization to evaluate their own unique privacy risks and address them appropriately. This guide will help by providing time-saving tools and guidance.

What this guide can do for you

Taking privacy precautions is more than important; it is an essential and inevitable component of business success. Serious consequences to an organization's goals and business success can result from inadequately and not continually addressing these risks. Following a well-thought-out privacy and security assurance and governance program will help an organization successfully and effectively choose the types of privacy risks they are willing to reasonably tolerate and decide which others must be effectively addressed. This guide will help you:

- Determine where you currently are with regard to privacy governance maturity
- Take corrective action to fill gaps with privacy activities that you need to be performing
- Maintain an effective and efficient privacy governance program

- Save time by outlining the components necessary for an effective privacy governance program.
- Identify gaps in your current privacy governance program
- Identify ways to sell privacy to your executives, business partners, and personnel
- Establish policies and procedures to demonstrate due care practices, and help lessen liability that may accompany civil actions or resulting from a privacy incident

Reason	Result
Expand privacy activity budget and add more personnel.	Documented privacy governance programs and associated process shows management what is needed.
Establish top management communication path.	Participation of management in a privacy governance program establishes necessary support.
Establish privacy governance effort credibility and visibility.	A privacy governance program will be well documented and had the sign-off of the executive officer's signature on the cover page.
Shift worker attitudes and change perspectives.	The support of all personnel who interact with personally identifiable information systems is mandatory and now it's in writing.
Harmonize and coordinate the activities of many personnel.	Consistent action is necessary to achieve and maintain privacy.
Define the boundaries of permissible action.	Personnel will clearly understand how far they can go when personally identifiable information.
Control privacy-relevant events in advance.	Increases the chances that privacy incidents will be handled efficiently, appropriately and quickly.
Permit management to determine if personnel are acting appropriately.	Personnel should not fact the same disciplinary actions if they made a mistake as opposed to acting intentionally.
Avoid disputes and related	Because privacy activity roles are clearly defined,

internal politics.	personnel can focus on business problems instead of who is responsible for privacy and how to handle privacy issues.
Enable rapid development of new systems.	Define as many of the privacy requirements in advance so they will not need to be revisited for every project.
Coordinate activities of internal and external groups.	A formal privacy governance program will help to ensure activities are not duplicated in conflict with each other, and will also help ensure gaps are not left un-addressed.
Achieve lower costs through privacy activities standardization.	The same approach for addressing similar privacy requirements can be used consistently throughout the organization.
Prevent all decentralized groups from “reinventing the wheel”.	By specifying privacy requirements and activities centrally, distributed groups need not develop them.
Demonstrate internationally accepted privacy practices are used within you organization.	The Organization for Economic Cooperation and Development (OECD) recommends all organizations adopt a set of privacy requirements based upon their published recommendations.
Establish benchmarks or reference points for future audits.	Internal auditors can determine whether compliance exists.
Guide privacy product, and service selection and implementation.	Uncoordinated dispersed groups are less likely to make decisions that are in conflict with the organization’s requirements.
Demonstrate compliance with laws and regulations	A documented privacy governance program provides evidence of management support and documents privacy requirements.
Arrange contractual obligations needed for prosecution.	Use privacy compliance agreements and confidentiality agreements, non-compete agreements, and related documents to create legal obligations.

Using this guide

This guide is designed to help your organization more effectively manage the resources required to protect the confidentiality and privacy of the personally identifiable data you collect, handle, store and process in any form. Within this guide I refer to this practice as “Privacy Governance.” If you currently have a privacy governance program in place, this guide will help you become more effective by providing information and tools critical to your success. If you are just starting to deal with privacy in your organization, and do not have a formal program in place, this guide will help you get started in an organized fashion. The information, resources, tools and templates of this guide should save your organization many hours of detailed labor. The following table is an overview of this guide and how it can be used to manage a privacy governance program.

Chapter	Overview
Chapter 1: Privacy Impact on Business	This chapter discusses the overall need to establishing a privacy governance program, including many recent fines and sanctions as a result of privacy breaches. Organizations in which senior management is not aware of privacy issues can use this data to help build a case for establishing a formal program.
Chapter 2: Creating a Privacy Governance Program	Chapter 2 describes the core elements of a privacy governance program, including reasons why each element is critical to compliance with international laws. Chapter 2 lists several key policies that should be included in the organization’s internal privacy policies.
Chapter 3: Defining Personally Identifiable Information	Chapter 3 provides a roadmap for organizations to properly define Personally Identifiable Information for its customers. This is a crucial first step in any privacy program.
Chapter 4: OECD Privacy Principles	Chapter 4 discusses the privacy principles established by the Organization for Economic Cooperation and Development (OECD). These privacy principles are used as the basis for many of the laws and regulations discussed in Chapter 5 and Chapter 6 . This chapter also provides pre-written policies that address each of the detailed data protection requirements of the

	OECD principles.
Chapter 5: U.S. Privacy Related Laws	Chapter 5 describes a number of laws that effect data privacy requirements for US citizens. Most organizations that do business within the United States will need to comply with one or more of these laws.
Chapter 6: International Privacy Related Laws	Chapter 6 describes a number of critical data protection laws outside of the United States. These laws generally apply to data collected on non-US citizens. This chapter is especially useful to international companies who must be concerned with personal data flow across international borders.
Chapter 7: Privacy Enhancing Technologies	Chapter 7 describes a number of important technologies used to enhance data privacy. Chapter 7 includes a discussion of each technology, including samples policies for organizations that must use these technologies. A number of the laws referenced in Chapter 5 and Chapter 6 require the use of privacy enhancing technologies.
Chapter 8: Privacy Inhibiting Technologies	Chapter 8 describes a number of important technologies that can be used to inhibit or decrease privacy. Many organizations already deploy these technologies without understanding their privacy implications. Chapter 8 also includes sample policies for organizations to consider when managing privacy inhibiting technologies (PITS).
Appendix A: Privacy Glossary	Appendix A provides a glossary of terms used in this guide. This Appendix will be helpful to organizations who must document terms used in their internal policies and procedures.
Appendix B: Privacy Resources	Appendix B is a list of resources useful to privacy management professionals. Resources include professional organizations, web sites, books and other research material.
Appendix C: Privacy Officer Checklist	Appendix C provides a summary worksheet of tasks that should be done by the official responsible for privacy within the organization. This worksheet is

	provided in spreadsheet format for each customization or import into a project management software program.
Appendix D: Sample CPO Job Description	Appendix D provides a detailed discussion of the requirements for a Chief Privacy Officer or similar lead privacy role. Organizations can use this as the basis for their own internal documentation, or in establishing requirements for hiring a privacy professional to lead the organization.
Appendix E: Sample Privacy Incident Response Form	Effective privacy governance requires organizations to manage and respond to privacy-related incidents. Appendix E provides a sample privacy incident response form that organizations can easily customize for their own use.
Appendix F: Privacy Breach Impact Worksheet	Appendix F includes a spreadsheet that organizations can use to estimate the impact of a privacy breach. This type of analysis is critical for doing internal risk assessments related to privacy protection. An example of such an analysis is included earlier in this chapter.
Appendix G: Privacy Impact Self-Assessment	Appendix G provides a detailed Privacy Impact Self Assessment (PIA) based on the OECD privacy principles. The PIA form is in a separate Microsoft Word document that can easily be copied and filled out for your organization. PIAs are a critical part of the privacy governance process and required by several privacy laws.
Appendix H: Executive Privacy Presentation	Appendix H provides a Powerpoint presentation that organizations can use to educate executive management on the need for proper privacy governance.
Appendix I: Sample External Privacy Policy	Appendix I provides a sample external privacy policy, including discussions for customization based on the privacy principles discussed in this book. This sample external privacy policy is also available as a separate document.
Appendix J: Sample Employee	Appendix J provides a sample questionnaire that you

Privacy Awareness Assessment	can use to assess the overall awareness of your employees on data privacy issues. Organizations are encouraged to customize this quiz with issues specific to their data privacy requirements. This quiz can easily be posted on an intranet or included as part of an organization's learning management system (LMS).
------------------------------	---

Using the Sample Policies and Forms

The forms, policies and procedures provided in this guide are in generic form. They need to be customized to fit your own specific business environment, industry and geographic locations. To accomplish this:

- Involve your legal counsel, Human Resources representative, information security officer and privacy officer.
- Each individual providing input must have a good understanding of the business and privacy issues related to his/her responsibilities.

Please note: This Toolkit does not represent legal counsel or legal interpretation. It is provided as a guide to help information security, privacy and compliance professionals to start identifying the many types of personal information referenced within multiple laws that are considered as personally identifiable information. Each organization should use this as a starting point to confirm the interpretations as presented here.

Balancing Trade-Offs

Because this reference guide covers the wide spectrum of privacy issues, including those found throughout the world, you will see that some recommended practices may contradict each other. Each organization needs to establish the scope of their privacy governance program and use the information within this guide accordingly. What will work well for one company, even in the same industry, will not be the best plans for another company to use based upon many different variables, such as geographic locations, services and products, customers, business partners, and so on.

Establishing a privacy governance program will involve tradeoffs. There are many conditions and limits involved with privacy issues, and an effective privacy governance program must be designed with these in mind. For example, establishing retention requirements for PII will need to be based upon not only technology constraints, but also very importantly upon consideration of legal, regulatory and policy requirements.

The intention of this guide is to provide a source for you to use of the full range of privacy issues facing organizations, and provide recommendations for how to effectively implement your own privacy governance program. The logical inconsistency between some policies is also a reflection of the fact that there is no standard set of specific policies to which all organizations must subscribe. Instead, a set of policies must be uniquely tailored to the requirements of each organization.

Need For Competent Advice

It is imperative when establishing a privacy governance program for you to consult closely with your privacy officer, legal counsel, information security officer and human resources representative. Before implementing any privacy-related policy or procedure discuss them with this core of experts to ensure that all applicable laws and regulations are addressed, and that the proposed activities are feasible from a technology standpoint. There will also be times when you need to get assistance from the subject matter experts from within, and sometimes even outside, your organization. For example, if you are implementing privacy practices in a European country, be sure you obtain the feedback of personnel located within that country who are knowledgeable about the corresponding country laws and related business issues.

