CYBERCRIME & SECURITY

Compiled & Edited by
Pauline C. Reich

IV. NATIONAL LEGISLATION AND COMMENTARY

G. North America

Booklet IVG.United States.A-6

Collaboration: The Key to the Privacy and Security Balancing Act

by Rebecca Herold

Release 2010-1
Issued March 2010

Oceana®
NEW YORK

OXFORD
UNIVERSITY PRESS

Oxford University Press, Inc., publishes works that further Oxford University's objective of excellence in research, scholarship, and education.

Published by Oxford University Press, Inc.
198 Madison Avenue, New York, New York 10016

Oxford is a registered trademark of Oxford University Press
Oceana is a registered trademark of Oxford University Press, Inc.

Library of Congress Cataloging-in-Publication Data

Cybercrime & security / compiled and edited by Pauline C. Reich.
p. cm.
Includes bibliographical references.
ISBN: 978-0-379-1281-1 (looseleaf: alk. paper)
1. Computer crimes. 2. Computer security I. Reich, Pauline C.
HV6773.C92 1998
346.16'8d—c21 98-14524
CIP

Collaboration: The Key To The Privacy and Security Balancing Act

Rebecca Herold

About the Author
Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI

rebeccaherold@rebeccaherold.com
http://www.theprivacyprofessor.com
http://www.realtime-itcompliance.com
http://twitter.com/privacyprof
http://www.compliancehelper.com

Rebecca Herold, CIPP, CISSP, CISM, CISM, FLMI, "The Privacy Professor,"® has over two decades of information security, privacy and compliance experience. She's been named as a *Computerworld* "Best Privacy Advisor" multiple times, and also as a "Top 59 Influencers in IT Security" by *IT Security* magazine. The program Rebecca created was awarded the 1998 CSI Information Security Program of the Year Award. She is also currently the NIST Smart Grid Privacy Subgroup leader.

Rebecca assists organizations of all sizes and industries throughout the world. Rebecca is working on her 14th book, writes multiple monthly columns, creates the quarterly "Protecting Information" multi-media information security and privacy awareness subscription news journal and provides effective information security and privacy tools and online training courses. She also has served as an Adjunct Professor for the Norwich University Master of Science in Information Assurance (MSIA) program since 2004. You can reach her at rebeccaherold@rebeccaherold.com.

Privacy requires the implementation of information security controls and appropriate safeguards. Multiple units within an organization must work together to be effective and successful.

The need for convergence is nothing new

There has been much written in just the past few years regarding a convergence of information security and privacy. However, this convergence has actually existed ever since privacy became a concern. After all, you cannot have privacy without implementing security controls and appropriate safeguards.

I first experienced this firsthand during the first half of the 1990's when I was responsible for information security in a large multinational insurance and financial company based in the United States. The company launched one of the very first online Internet banks, and as I was establishing the security requirements I saw the need to address the privacy aspects. This was before the passage of the Gramm Leach Bliley Act (GLBA)[1] or the Health Insurance Portability and

1 See the full text of the Gramm Leach Bliley Act at http://www.ftc.gov/privacy/glbact/glbsub1.htm

Accountability Act (HIPAA)[2], but bills addressing privacy had been being considered, not only in the U.S. but also worldwide, and Organization for Economic Cooperation and Development (OECD) privacy principles[3] were the basis for most of the privacy requirements. I convinced the executives to post a privacy policy, based upon the OECD privacy principles, even though at the time law did not require it. After all, we needed to obtain and maintain customer trust, but could not effectively do so in the long term without establishing security controls that supported customer privacy.

An Historical Perspective

The assignment of a privacy officer became a legal requirement in the U.S. with the passage of HIPAA in 1996 and then again with Gramm Leach Bliley in 1999. This got the attention of organizations that had to comply with the laws, and they typically enlisted their existing VPs in the Legal or Marketing areas to fulfill these requirements.

The Information Security profession emerged in the mid-1970's as a technical field, often seen as a mainframe security access gatekeeper, such as the TopSecret and RACF[4] security administrator.[5] Information Security really started to move up in importance during the beginning of the client/server era. In the mid-1990's, more corporate Information Security positions were created than ever before. It wasn't until the laws and regulations requiring assignment of Information Security responsibility and accountability that the position started to move upward in the organization because it was then viewed as a business responsibility and not just something nice to have, or necessary to keep the computer systems available and functioning.

Convergence issues

Throughout the years I have identified over twenty business areas and activities where Information Security and Privacy responsibilities and activities converge. More areas continue to emerge as technology, laws and business evolve. As just one example, the Information Security and Privacy functions in all types of organizations, both privacy and public, must work together to effectively understand and comply with the multiple requirements in the (at least) 48 U.S. state and territory privacy breach notice laws[6] in a unified manner throughout the enterprise.

---

2 See the full text of the Health Insurance Portability and Accountability Act at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf

3 See the OECD privacy principles at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

4 Top Secret and RACF ((Resource Access Control Facility) are software products used for access control management in computer systems.

5 Abramson, Christopher. "A Return to Legacy Security." July 27, 2001, pg. 3, <http://www.sans.org/reading_room/whitepapers/mainframes/a_return_to_legacy_security_247> (Oct. 31,2009).

6 See a list of the U.S. state and territory breach notice laws as of October 2009 at http://www.privacyguidance.com/elegal_regulations.html and see Perkins Coie chart in this release at IVG.United States.C-7.

There are growing numbers of incidents, accompanied by growing numbers of fines, penalties and civil actions. At the core of compliance for these hundreds of laws and regulations is:

1) Knowing the information that is to be considered as personally identifiable information (PII), as well as personal information, within the organization,

2) Knowing where this personal information is collected, stored, and leaves the organization, and

3) Establishing effective safeguards to protect this personal information throughout the entire information lifecycle.

Privacy is not a strictly legal issue, and information security is certainly not a strictly technical issue; they intersect in many ways. To effectively manage, protect and appropriately use and share personal information, all areas of an organization must work together.

Overlapping Areas

There are growing numbers of business issues where Information Security and Privacy activities and responsibilities overlap. Table 1 provides a list (in no particular order, but enumerated simply to make referencing easier) of the areas that I have identified throughout the past two plus decades I have been doing Information Security, Privacy and compliance work.[7] As time goes by, this list will change as new issues are added and others may drop off as they become obsolete.

Information Security and Privacy Overlaps

1. Laws, regulations and standards
2. Business frameworks and "Governance, Risk management and Compliance" (GRC)
3. Outsourcing and third party controls
4. Security incident and privacy breach response plans
5. Privacy and security training and awareness
6. Increased use of mobile computing
7. Risk management activities
8. Privacy and security scorecards and metrics
9. Customer relationship management (CRM) and data mining
10. Web 2.0 use
11. Cloud computing
12. Encryption

7 For more detail about these , *see* "Unified Information Security and Privacy Management;" at http://www.privacyguidance.com.

13. Certifications and trust seals
14. Record retention and e-discovery
15. Information disposal
16. Cyber risk insurance
17. Employee monitoring and checks
18. Data inventories and data flows
19. Business resiliency and pandemic planning
20. Policies and procedures
21. Systems and applications development

Table 1 – Privacy and Information Security Overlapping Issues[8]

Laws, regulations and standards

There are literally hundreds of data protection and privacy laws, regulations and standards worldwide. Listing them all would fill many pages. Table 2 provides a representative sample of many of the U.S. laws, regulations and standards that Information Security and Privacy leaders must work on together to effectively meet the many and varied requirements. Table 3 provides a representative sample of international data protection laws.

U.S. Privacy and Data Protection Laws and Regulations

- Children's Online Privacy Protection Act (COPPA)
- Communications Assistance for Law Enforcement Act (CALEA)
- Electronic Communications Privacy Act (ECPA)
- Fair Credit Reporting Act (FCRA, PDF)
- Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- FACTA's Red Flag Rule
- FACTA's Disposal Rule
- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Trade Commission (FTC) Act
- Health Insurance Portability and Accountability Act (HIPAA)
- HITECH Act

8 As determined by research performed by Rebecca Herold; http://www.privacyguidance.com.

- At least 48 state-and territory-level breach notice laws
- Many assorted state and territory credit freeze, medical privacy, and other privacy-impacting laws

Table 2 – U.S. Data Protection Laws and Regulations[9]

International Privacy and Data Protection Laws and Regulations

- EU Data Protection Directive 1995/46/EC
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- Australia Federal Privacy Act
- Japan's Law on the Protection of Personal Information

Table 3 – International Data Protection Laws and Regulations[10]

9 Children's Online Privacy Protection Act (COPPA) see http://www.ftc.gov/ogc/coppa1.htm Communications Assistance for Law Enforcement Act (CALEA) see http://www.fcc.gov/calea/

Electronic Communications Privacy Act (ECPA) see http://commdocs.house.gov/committees/judiciary/hju67343.000/hju67343_0.htm

Fair Credit Reporting Act (FCRA) see http://www.ftc.gov/os/statutes/fcra.htm

Fair and Accurate Credit Transactions Act of 2003 (FACTA) see http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf

FACTA's Red Flags Rule see http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf

FACTA's Disposal Rule see http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf

Family Educational Rights and Privacy Act (FERPA) see http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Gramm-Leach-Bliley Act (GLBA) see http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

Federal Trade Commission (FTC) Act see http://www.ftc.gov/ogc/ftcact.shtm

Health Insurance Portability and Accountability Act (HIPAA) see http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

HITECH Act see http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

At least 48 state-and territory-level breach notice laws see http://www.privacyguidance.com/files/USStateTerritoriesBreachNotificeLawsasof07.20.09.pdf

Many assorted state and territory credit freeze, medical privacy, and other privacy-impacting laws see http://www.privacyguidance.com/elegal_regulations.html

10 EU Data Protection Directive 1995/46/EC see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) see http://www.priv.gc.ca/legislation/02_06_01_e.cfm

Australia Federal Privacy Act see http://www.privacy.gov.au/law/act

Table 4 lists some of the internationally accepted privacy and information security principles that can be used as a basis for creating information security and privacy program programs.

Internationally-Accepted Information Security and Privacy Standards
• Organisation for Economic Cooperation and Development (OECD) Privacy Principles
• American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP)
• ISO 27001 and ISO 27002 Information Security Standards

Table 4 – Privacy and Information Security Standards[11]

CEOs and other business executives are increasingly concerned, and actively engaged, in implementing initiatives to ensure their organizations are achieving compliance with all their regulatory, contractual, industry standards, and policy obligations.[12] This is a welcome change from just a few years ago, when it was very hard to get Information Security projects, that impact privacy compliance in so many different ways, approved.

Business frameworks and GRC

Information Security and Privacy areas have many opportunities to integrate their compliance requirements into a growing number of frameworks increasingly used by organizations. Information Technology (IT) departments are increasingly using the IT Infrastructure Library (ITIL) framework[13] to help ensure IT systems and applications best meet and support business goals and initiatives. Internal audit departments are using the Control Objectives for Information and related Technology

---

Japan's Personal Information Protection Act see http://www.zlti.com/resources/docs/Rules%20and%20Regulations/ZL.RR.Japan-PIPA.pdf

11 Organisation for Economic Cooperation and Development (OECD) Privacy Principles see http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html

American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP) see http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Generally+Accepted+Privacy+Principles/

ISO 27001 and ISO 27002 Information Security Standards see http://www.27000.org/

12 According to a July 2009 Ponemon study, "The Business Case for Data Protection," sponsored by Ounce Labs, complying with data protection and privacy laws was rated as "important" to "very important" to 64% of the CEOs, but only 33% of the other C-level business leaders. See the full report at http://www.ouncelabs.com/PonemonStudy2009.

13 According to the site, "…the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally." For more information see http://www.itil-officialsite.com/home/home.asp.

(COBIT®)[14] framework as a basis for evaluating enterprise controls. Integration of frameworks is an effective strategy to address regulatory compliance throughout the enterprise. Governance, Risk Management and Compliance (GRC) is the latest buzzword expression used to describe this enterprise-wide collaboration to identify and mitigate risks along with addressing compliance requirements.

Using business frameworks between the departments, teams and positions with responsibilities for risk mitigation, regulatory and legal compliance and privacy preservation allows them to build common solutions. Using frameworks helps to ensure consistency throughout the enterprise with these efforts, makes the work activities more efficient and effective, and demonstrates due diligence, all of which communicate the credibility of the Information Security and Privacy program to internal auditors, external auditors regulatory examiners, business partners, customers and consumers. Additionally successfully using frameworks to address Information Security and Privacy can provide a competitive advantage to business organizations by helping them to demonstrate to consumers their commitment to protecting personal information, resulting in improved brand reputation.

Additionally, using frameworks helps all kinds of organizations to manage the increasing complexity of Information Security and Privacy issues. Increasing number of new laws, constantly new and emerging technologies, and continuously growing numbers of threats make managing Information Security and Privacy threats more and more challenging. Add to this the loud demands of consumers and stakeholders for more transparency of Information Security and Privacy operations, controls, processes, costs, compliance and diligence, and it becomes clear that using frameworks helps to link Information Security and Privacy activities closely to the business and gives a better understanding of related activities to customers and stakeholders.

Frameworks Supporting Privacy and Security

- ITIL is being used to address information technology risks[15]
- COBIT[16] is being used to address audit and control risks

14 According to the ISACA site, COBIT "…provides good practices across a domain and process framework and presents activities in a manageable and logical structure." For more information see http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

15 According to the site, "...the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally." For more information see http://www.itil-officialsite.com/home/home.asp.

16 According to the ISACA site, COBIT "...provides good practices across a domain and process framework and presents activities in a manageable and logical structure." For more information see http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

- ISO/IEC 27001 and ISO/IEC 27002 are being used to address information security risks[17]
- OECD/GAPP principles are being used to address privacy risks[18]

Table 5 – Frameworks supporting privacy and information security

When Information Security and Privacy units collaborate and build their programs around proven and consistent frameworks, they:

- Establish common solutions for multiple compliance areas
- Are more efficient and convey credibility of the programs to auditors and regulatory examiners
- Provide a competitive advantage by improving customer confidence and increasing brand reputation

Outsourcing and third party controls

More businesses are outsourcing than ever before. According to an August 2009 Cutter report, global offshore outsourcing market revenues for IT and business services exceeded US $55 billion in 2008, and some estimates suggest an annual growth rate of 20% over the next five years[19]. More and more services and business processes are being outsourced to Brazil, Russia, India, and China, viewed as the "BRIC" inheritors of globalization and offshore outsourcing. Organizations that are not outsourcing offshore are increasingly outsourcing specific types of business activities to business partners within the same country.

As more and more business processing is outsourced, there are also more and more Information Security and Privacy incidents occurring with business partners than ever before. Organizations cannot shrug off their responsibilities for ensuring their business partners have effective security and privacy controls in place. Organizations remain responsible for the security of the information they collect from customers and personnel even when they hand it off to other businesses. Industry-specific regulations such as GLBA and HIPAA require that vendor security be validated. Now, under the U.S. HITECH Act expansion of HIPAA[20], such

17 ISO 27001 and ISO 27002 Information Security Standards see http://www.27000.org/

18 Organisation for Economic Cooperation and Development (OECD) Privacy Principles see http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html

American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP) see http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Generally+Accepted+Privacy+Principles/

19 Accessed October 28, 2009 from http://www.cutter.com/content/alignment/fulltext/reports/2009/08/#notes

20 HITECH effectively expands Privacy Rule and Security responsibilities for HIPAA to all business associates (BAs) of covered entities (CEs). Additionally, HITECH requires CEs

vendor validation requirements are even more clearly established. For example, the HITECH Act greatly expanded HIPAA requirements to business associates, and covered entities must take actions to ensure the business associates are in compliance with security and privacy requirements.

Growing outsourcing, along with integration of networks with customers, suppliers, and business partners, such as through cloud computing[21], blurs the traditional definition of the corporate perimeter. Organizations must document the activities and processes implemented to ensure business partners have appropriate security and privacy controls in order to demonstrate due diligence as well as to prevent breaches from occurring within business partners because of poor or missing controls.

It is important to create a documented process to consistently manage vendor and business partner relationships and ensure all business partners and vendors are appropriately protecting the information and systems entrusted to them[22]. This process must include the privacy expectations as well as the information security requirements. Organizations will be able to achieve effective business partner management by using a consistent approach, along with supporting tools and techniques.

Over a two-year period, from 2005 to 2006, the author did approximately two hundred (200) business partner security and privacy program reviews for a number of large multinational financial and healthcare insurer organizations. The author was able to do all these reviews consistently, efficiently and effectively by using a well-thought-out procedure with supporting tools she developed that included consideration of both Information Security and Privacy issues. The author consistently found similar bad Information Security and Privacy practices within those business partners that put the financial and healthcare insurer organizations at great risk. Some of the common problems included:

- No formally documented information security or privacy responsibilities
- Information security and/or privacy positions reporting too low within the organization to have effective authority
- No documented Information Security or Privacy policies and procedures
- No documented awareness and training requirements or programs
- No requirements for encryption on mobile computing devices

---

and BAs to have breach identification and response plans in place, along with training and awareness for personnel.

21 The term "cloud computing" basically means that business services and processing (such as applications, software and hardware) are being sent outside the corporate network to Internet-based servers that are also providing the same services for other businesses. Generally, cloud computing involves other organizations providing dynamically scalable and often virtualized software and hardware resources as a service over the Internet.

22 For an example of a cloud computing service I've created to monitor business partner and vendor Information Security and Privacy program compliance, *see* http://www.compliancehelper.com.

- No requirements for encryption on confidential information sent through public and untrusted networks
- No documented disaster recovery or business continuity plans, or old plans that had never been updated or tested
- No regular reviews of the internal network for vulnerabilities
- No regular external network vulnerability/penetration tests

The bottom line is that business partner Information Security and Privacy practices impact one's own organization's reputation. An organization's business partners' security and privacy risks are also the organization's risks; the organization is only as secure as its weakest link.

Information Security and Privacy functional units can collaborate and build their programs to address vendor and business partner risks by partnering on:

- Contracts
- Business partner and vendor self-assessment forms and questionnaires
- Network perimeter scans
- Third party audits and reviews
- Internal measures taken to protect against real or perceived partner weaknesses

Security incident and privacy breach response plans

The increased risk of unauthorized access to systems and data, as well as the increase in legislative mandates for protecting private data and responding to privacy breaches, makes establishing an Information Security incident and Privacy breach response plan a necessity within every type of business organization. Table 6[23] provides a listing of the 48 U.S. state and territory level breach response laws that were in effect in October 2009.

U.S. State & Territories Breach Notification Laws as of July 20, 2009

1. Alaska HB 65
2. Arizona SB 1338
3. Arkansas SB 1167
4. California SB 1386 & AB1298
5. Colorado HB 1119
6. Connecticut SB 650
7. Delaware HB 116

23 Taken from "**U.S. State & Territories Breach Notification Laws as of July 20, 2009**" accessed October 12 2009 at http://www.privacyguidance.com/elegal_regulations.html.

8. District of Columbia "§ 28-3852
9. Florida HB 481
10. Georgia SB 230
11. Hawaii SB 2290
12. Idaho SB 1374
13. Illinois HB 1633
14. Indiana HB 1101
15. Iowa SF 2308
16. Kansas SB 196
17. Louisiana SB 205
18. Maine LD 1671
19. Maryland HB 208 & S.B. 194
20. Massachusetts HB 4144
21. Michigan SB 309
22. Minnesota HF 2121
23. Missouri HB 62
24. Montana HB 732
25. Nebraska LB 876
26. Nevada SB 347
27. New Hampshire HB 1660
28. New Jersey A4001
29. New York S 3492, S 5827 & AB4254
30. North Carolina SB 1048
31. North Dakota SB 2251
32. Ohio HB 104
33. Oklahoma HB 2357
34. Oregon SB 583
35. Pennsylvania SB 712
36. Puerto Rico HB 1184, Law 111
37. Rhode Island HB 6191
38. South Carolina SB 453, Act 190

39. Tennessee HB 2170
40. Texas SB 122
41. Utah SB 69
42. Vermont SB 284
43. Virgin Islands VI Code § 2209
44. Virginia SB 307, Chapter 566
45. Washington SB 6043
46. West Virginia SB 340
47. Wisconsin SB 164
48. Wyoming SF 53

Table 6 – U.S. state and territory breach notice laws[24]

Table 7 lists a few of the U.S. federal breach notice laws.

Sample U.S. Federal Breach Notice Laws and Regulations

- HITECH Act
- FISMA
- E-Government Act
- FTC Act

Table 7 – Sample U.S. federal breach notice laws[25]

As of November 2009, there were also many existing and proposed breach notice laws and guidelines throughout the world. Table 8 provides an example of some from countries outside the U.S.

24 As documented by Rebecca Herold at http://www.privacyguidance.com/files/USStateTerritoriesBreachNotificeLawsasof07.20.09.pdf

25 HITECH Act see http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

Federal Information Security Management Act (FISMA) http://csrc.nist.gov/groups/SMA/fisma/index.html

E-Government Act see http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2458.ENR:

FTC Act (indirectly; if an organization's policy states it will detect and report breaches, then it is legally obligated to do so) see http://www.ftc.gov/ogc/ftcact.shtm

Sample Worldwide Breach Notice Laws, Bills and Guidelines

- European Union: EU Data Protection Directive Article 29[26]
- Hong Kong: Hong Kong: Code of Practice on Consumer Credit Data (2003)[27]
- India: Information Technology Act, 2000 (as amended by Information Technology Act, 2008)[28]
- Ireland: Data Protection Commissioner Breach Notification Guidance[29]
- Germany: *Bundesdatenschutzgesetz* (Federal Data Protection Act, "BDSG" or the "Act")[30]
- Canada: Office of the Saskatchewan Information and Privacy Commissioner Privacy Breach Guidelines[31]

Table 8 – Sample worldwide breach notice laws, bills and guidelines

Incident and breach plans will be ineffective if Privacy and Information Security functional areas do not collaborate on the plans. There will be gaps created if each area assumes the other area is addressing an important issue; and with lack of collaboration between the areas, this will happen. There will be conflicts if multiple units try to create controls and plans to address the same issues.

Information Security and Privacy units can collaborate and build their programs to address breach notice responsibilities by partnering on:

- Identifying all legal requirements for breach notifications
- Auditing, logging,monitoring, and intrusion detection systems
- Establishing Information Security incident and privacy breach response plans and teams
- Training incident and breach response team members.

26 Accessed October 12, 2009 from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf

27 Accessed October 23, 2009 from http://www.pcpd.org.hk/english/files/ordinance/CCDCode_eng.pdf

28 Accessed November 15, 2009 from http://www.cyberlawtimes.com/itact2008.pdf

29 Access November 17 ,2009 from http://www.dataprotection.ie/viewdoc.asp?DocID=901

30 Accessed November 2 ,2009 from http://www.thefreelibrary.com/Germany+Strengthens+Data+Protection+Act,+Introduces+Data+Breach...-a0211022159

31 Accessed November 1, 2009 from http://www.oipc.sk.ca/Resources/Privacy%20Breach%20Guidelines1%20(3).pdf

Privacy and Information Security training and awareness

People are the weakest link in security and privacy assurance; it is critical they have the knowledge to use information resources securely and in a way to protect privacy.

Imagine this: What if you were given training just once, in a 1-hour session with no hands-on practice, for how to do first aid and give CPR and then were never given more training or reminders about how to do first aid and CPR. Two years later would you be able to competently perform first aid when someone needed it? Probably not. Probably not even 1 year later, or even 6 months later.

People need to have regularly scheduled training and ongoing awareness in how to carry out activities competently. You cannot expect to give a 1-hour, often poorly-constructed, training course about Information Security or Privacy and then have the people taking the training know what to do weeks or months or even yeas later, however, this is the situation that occurs in a very large majority of organizations.

It is no wonder that the majority of security incidents and privacy breaches occur as a result of lack of knowledge and mistakes.

An effective Information Security and Privacy awareness program must communicate to personnel, outside of the formal training sessions, the importance of observing and maintaining Information Security and Privacy as well as motivate personnel to learn and follow the organization's Information Security and Privacy policies and procedures. Personnel must receive ongoing communications about the situations they deal with every day that involve Information Security and could result in privacy breaches.

These ongoing communications should occur in a variety of ways to help ensure that personnel know and understand the importance of properly following Information Security and Privacy procedures. Tailoring awareness communications and activities to one of the following three types of learners can truly educate all of an organization's personnel:

- Visual—These are the folks who learn best through seeing and reading.
- Audio—These folks learn best by listening to information.
- Kinesthetic—These are hands-on learners; those who need to do some type of activity to learn.

Over the years, I have accumulated and documented more than 200 types of information security and privacy awareness communications and activities for businesses to use.[32] The number of possibilities is only limited by your imagination.

32 Some are available online and others are provided in my book Managing an Information Security and Privacy Awareness and Training Program. published by Auerbach in 2005. The

Not only is ongoing training and awareness necessary for effective Information Security and Privacy, there are numerous legal requirements for privacy and information security education as part of compliance. Probably the most commonly discussed regulations in the U.S. are the Health Insurance Portability and Accountability Act (HIPAA)[33], the Sarbanes–Oxley Act (SOX)[34], and the Gramm–Leach–Bliley Act (GLBA)[35], however, personnel education has been a requirement under other guidelines and regulations for several years. For instance, the Federal Sentencing Guidelines[36] enacted in 1991, used to determine fines and restitution for convictions, have seven requirements, one of which is for executive management to educate and effectively communicate to their employees the proper business practices with which they must comply.

Information Security and Privacy units can collaborate and build their programs to address training and ongoing awareness communications and activities by partnering on:

- Creating a training and awareness activities schedule
- Creating training content
- Sponsoring awareness events
- Establishing ongoing education effectiveness metrics
- Budgeting for training and awareness resources

Increased use of mobile computing

Consider the following statements:

- More mobile computing devices are used than ever before, and the numbers are increasing.
- More types of mobile storage media are used than ever before, and the numbers are increasing.
- More personnel are doing business work on mobile devices than ever before.
- More personnel are doing business work while outside business facilities than ever before.

2nd edition of the book will be released in 2010.

33 See http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

34 See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf

35 See http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

36 See http://www.ussc.gov/guidelin.htm

- More privacy and security incidents involve mobile computing devices and storage media than ever before, and the numbers are increasing.
- Mobile computing devices and mobile storage media threaten Information Security and Privacy more than ever before.

Most organizations got into mobile computing at the hands of the folks in the various business units, and security was an afterthought. By the end of 2009, 70% of the workforce in the U.S. qualified as being "mobile" at least some of the time.[37] Recent history has shown numerous incidents and privacy breaches have occurred as a result of not properly addressing mobile computing security. Just a couple of examples include:

- Reported December 15, 2009: The Beijing Center for Chinese Studies reported a laptop containing a large number of names and Social Security numbers for study abroad students was stolen.[38]
- Reported December 21, 2008: Connecticut Department of Motor Vehicles notified customers that their personal information was on a computer stolen from a mobile service center vehicle while it was being repaired. Personal data on the computer included names, addresses, date of birth, license numbers, photos and signatures of at least 155 individuals.[39]

It's no wonder, considering that mobile computing and storage devices have become indispensable tools for today's highly mobile workforce. But they:

- Can be easily lost or stolen, resulting in the potential breach of personal or sensitive data,
- Are subject to the downloading of spyware and malware that can infect an organization's computer network, and
- Are subject to eavesdropping through wireless access points,
- Can have communications intercepted, and
- Can be used to improperly track users.

37 According to an IDC Research Inc. (IDC) 2009 study: "By end of 2009, IDC estimates fully 70% of the U.S. workforce will qualify as 'mobile' at least part of the time." Accessed on November 12, 2009 from http://www.cfo.com/article.cfm/13981427/c_14020916

38 Accessed on December 24, 2009 from http://www.thebeijingcenter.org/securityqns.

39 Accessed on December 24, 2009 from http://www.ct.gov/dmv/cwp/view.asp?a=805&q=401094

Information Security and Privacy professionals need to work together to minimize the risks associated with mobile computing by personnel. A few of the collaborative efforts that can reduce risks include:

- Conducting a mobile computing risk assessment for both security and privacy risks
- Providing joint Information Security and Privacy training for mobile workers
- Establishing wireless computer and device configuration management controls
- Eliminating or disabling unnecessary applications downloaded onto mobile devices[40]
- Enabling the ability to remotely erase or lock access to data stored on mobile devices[41]
- Encrypting data on mobile computers and storage devices
- Requiring and installing firewall, anti-virus, intrusion detection, and anti-spam software on mobile computers used for business purposes

Risk management activities

A first step in business protection is to identify risks faced by the organization and to quantify the likelihood of their occurrence and the potential severity of their impact. An important activity that both Information Security and Privacy practitioners must ensure occurs is risk management. Based upon the results of risk assessments, appropriate corresponding controls must be established for those risks that are determined to be too great to accept within the business.

Risk assessments are legally required by multiple laws, such as, in the U.S., HIPAA, GLBA, the Federal Information Security Management Act (FISMA), and the Privacy Act, just to name a few. Other countries' laws also require safeguards to be implemented based upon an organization's risk, such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the EU Data Protection Directive. Any company processing credit cards must perform risk assessments under PCI DSS requirements. Guidelines used by auditors, such as COBIT 4.1, include requirements for risk assessment.

40 For example, such as instant messaging applications.

41 Growing numbers of applicatiosn and technology tools exist to track and remotely delete files from mobile devices remotely.

Table 9 shows a few excerpts from some of these that include the risk assessment directives.

Compliance Directive	Section	Risk Analysis Directive Excerpt
COBIT 4.1[42]	PO9.4 Risk Assessment	"Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis."
PCI DSS v1.2[43]	Appendix C Compensating Controls Worksheet	"Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance."
FACTA[44]	Sec. 114	"…identify possible risks to account holders or customers or to the safety and soundness of the institution or customers;"
HIPAA Security Rule[45]	Administrative Safeguards 164.308(a)(1)(ii)(A)	(ii) Implementation specifications; (A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Table 9 – Risk Analysis Requirements

Privacy practitioners should perform privacy impact assessments to identify, and then be able to effectively mitigate privacy risks. A PIA is a type of risk assessment, focusing on privacy issues, most effectively performed if based upon the Organisation for Economic Cooperation and Development (OECD) privacy principles. All U.S. government offices must perform annual PIAs, as do many government offices outside the U.S., such as those in Canada.

Privacy risk assessments and Information Security assessments will be more effective, more efficient, and reveal more issues, making them more valuable to the business, if they are done in partnership.

42 See http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=31519.

43 See https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

44 Fair and Accurate Credit Transactions Act of 2003 (FACTA) see http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf

45 Health Insurance Portability and Accountability Act (HIPAA) see http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

Privacy and security metrics

An increasing number of organizations are working to include Information.

Security and privacy metrics in their executive management scorecards.[46]

Finding creative ways to communicate risk in business terms will provide significant benefits when Information Security and Privacy units work together. The use of collaborative Information Security and Privacy metrics can:

- Communicate performance-Metrics can demonstrate the performance of your Information Security and Privacy initiatives. They help business leaders better understand the value of Information Security and Privacy.
- Drive performance improvement-Metrics can increase visibility to help personnel be more diligent. Information Security and Privacy metrics[47] to clearly communicate the many associated issues that are being addressed, and how successful those initiatives are.
- Measure the effectiveness of controls. Metrics can show whether or not Information Security and Privacy controls are producing the expected results. For example, are there few privacy complaints following a change to the posted privacy policy and staff training?
- Be used to diagnose problems. Metrics provide objective data to support Information Security and Privacy conclusions about vulnerabilities and threats.
- Provide effective decision-making support. Where are the greatest areas of opportunity for an organization to address as a matter of priority? What would be the expected result if an organization invested in a specific security project? More than just providing assistance with budget justification, a metrics program can facilitate objective data-driven decision-making.
- Provide increased accountability. Communicating Information Security and Privacy metrics can improve the efforts of the Information Security and Privacy teams. Different areas can compare results to an agreed-upon baseline or to industry baseline metrics. Such comparisons can dramatically increase motivation and improve compliance efforts.

46 Executive management scorecards is a current trend for communicating metrics for information security and privacy, along with other types of business measurements, to executive management. Typically the scorecards represent the key measurements as graphical representations of how well each specific initiative and/or responsibility is being managed or addressed.

47 There are many types of metrics that can, and are, being used by businesses to communicate the success of a wide range of information security and privacy initiatives. A couple of examples include 1) the amount of time it took to respond to and resolve a malicious code attack within the network, and 2) the number of customer privacy complaints received in a week.

- Guide resource allocation. Metrics can help to more accurately determine risk levels throughout the enterprise, justifying requests for more resources and funding.
- Demonstrate the state of compliance. Providing consistently calculated metrics can validate and demonstrate compliance with not only internal policies, but also established governance frameworks and regulatory requirements. Providing regular reports of metrics, from quarter to quarter, provides visibility to Information Security and Privacy efforts and also shows how well the organization is meeting compliance goals.

Customer relationship management (CRM) and data mining

There are several kinds of data mining: text mining, web mining, relational databases mining, graphic data mining, audio data mining and video data mining, which are all used in business intelligence applications to analyze consumer data.[48] Businesses and government agencies are using data mining increasingly more often in efforts to garner more business. For example, on December 22, 2009, the Los Angeles County Board of Supervisors approved using high-tech data mining solutions to detect child care benefits fraud.[49] There are both Information Security and Privacy issues involved with CRM and data mining activities.

For example, consider the free email accounts that many large companies, such as Microsoft and Google, offer. To get an account you must often submit your name, age, gender and ZIP code, and also agree to receive "targeted" marketing messages. While these items seem innocent enough, consider how they are used. CRM activities make use of data mining, which can log the times of each day when the accounts check their inboxes. Then, their data mining algorithms can quite easily tell, based on the zip code, the average incomes for the neighborhood. This all becomes quite valuable when florists are willing to pay large sums of money to email advertisements to people who earn nice incomes during lunch hours on special days such as Mother's Day and Valentine's Day. These CRM data mining methods are so sophisticated that most people don't even realize their online activities are being monitored in such a way; they don't realize that they "magically" received ads for items that they really wanted based upon the results of data mining activities.

48 There is a wide range of data mining algorithms being used. They can reveal a very wide range of personal information, such as the trends for the types of purchases certain demographics of individuals are making, the times when certain groups of individuals are using specific social media sites, and so on.

49 Accessed on December 26, 2009 from http://www.scpr.org/news/2009/12/22/la-county-use-data-mining-technology-combat-fraud/ "The $3.2 million, two-year contract to target fraud in CalWORKs child care program will use data mining technology to help predict fraud."

Web 2.0 use

"*Web 2.0 is generally a term, made popular after the first O'Reilly Media Web 2.0 conference in 2004, describing the emerging ways in which World Wide Web technology and Web designs can be used to enhance and make easier information sharing, creativity, and group collaboration. Web 2.0 services and technologies include such things as social networking sites, wikis, and blogs."*[50]

Personnel increasingly want to use technology for personal reasons while they are at work, bringing risks into the office that must be addressed. As just one example, consider the use of Twitter. In 2008, Twitter leaped to the attention of Internet users and was adopted by staggering numbers of individuals. As of the end of November 2009, there were more than 90 million Twitter accounts.[51] The market tracking firm HubSpot Inc. projects there are 5000 to 10,000 new Twitter accounts created every day. Do you know when these accounts are heavily used? Yes, while at work. And many of the posted Twitter messages contain confidential company information; a possibly significant business information leak. Add to this all the other "Web 2.0" technologies, and business leaders truly have some important decisions to make regarding this technology use within their business facilities, computers, and networks.

Chances are, personnel within an organization are participating in one of the popular social networking Web sites, such as Facebook or MySpace.[52] These sites are not inherently bad, however, those using them must consider the opportunities for other people on the sites to do bad things. Used appropriately, these sites can be quite informative and entertaining. Used inappropriately, though, they can be dangerous not only to a business but also to its personnel, their families and friends.

When personnel visit social networking sites from the business network or computer systems, they may unintentionally expose information about personnel, customers, or a company's business-sensitive documents. How? Others on the site may be using social engineering schemes and malicious code, through the many peer-to-peer (P2P) communications these sites use, to scoop up the organization's valuable business information.

Although a company may have software in place to prevent malicious code from damaging its network, this software may not prevent attacks or damage that can occur through P2P communications, such as instant messaging (IM), file sharing, or voice capabilities (Voice over IP, or VoIP). It is also easy for other malicious

50 Rebecca Herold, "Web 2.0 Privacy and Security FAQ," http://www.privacyguidance.com/files/CSI_Alert_October_2008.pdf, CSI Alert, October 2008

51 According to http://www.productweetity.com/

52 According to a March 2007 survey by security firm Clearswift, more than 75% of workers under 30 access social networking sites regularly from their work computers. Half of these say they have discussed their work, employer, customers, or coworkers on social networking sites.

software such as keyloggers and screenscrapers[53] to be loaded on a workstation while communicating with social networking sites. These malicious programs may be able to record every keystroke or use other methods to secretly steal sensitive corporate or customer information.

There are Information Security and Privacy concerns for all of these Web 2.0 capabilities. Organizations need to think about the threats Web 2.0 offerings bring to their organizations and determine the risks. To most effectively address all the risks, Information Security and Privacy functional units must work together to:

- Create strong Information Security and Privacy policies and procedures for using Web 2.0 technologies and sites while at work and while using business computers and networks.[54]
- Provide personnel with training and ongoing awareness for how to use them in appropriate ways that safeguard business, customer and employee information
- Identify and implement appropriate controls to keep bad things from happening as new Web 2.0 technologies emerge.

Cloud computing

"Cloud computing" floated across the IT horizon in 2008 to become one of the hot topics of conversation for most IT leaders. For those who may wonder, cloud computing is a nebulous term used to describe any of a number of services or applications that many businesses, as well as individuals, use that are actually located outside the network perimeter and on other entities' servers accessible via the Internet. They are very much like silent business partners.

Are those silent business partners securing their servers appropriately, and ensuring appropriate privacy protections to the vast amounts of personally identifiable information (personal information) that is being entrusted to them? Is there any need to worry? And what about how storing data on, and communicating via, clouds impacts compliance?

As companies start using more cloud computing resources for business purposes, business leaders will be wise to identify the sites and services they want to use, or may already be using, then review the Information Security and Privacy policies and update them accordingly to address these new risks. In addition to usage policies for employee interaction on public sites, companies must look for new ways to protect data on resources that are not under their direct control. This includes securing data as it is transmitted to and stored in the cloud, as well as granting the appropriate access rights regarding who can view the data. Organizations should

53 Screenscrapers are stealth computer programs that copy screen images and send to remote sites, all without the computer user even knowing that this copying activity took place.

54 For examples of such policies and procedures see "Web 2.0 Privacy and Security Considerations" written by Rebecca Herold at http://www.privacyguidance.com/files/CSI_Alert_October_2008.pdf

select cloud computing services carefully, and with their own legal requirements and their own Information Security and Privacy policies in mind.

Here are a few of the concerns with cloud computing, and associated questions, that Information Security and Privacy practitioners need to work together to answer:

- Where will the organization's data be stored?
- Will the organization's data be stored in a way that intermingles it with the data from other companies?
- Who has access to the information organizations are putting on these external cloud application and systems servers?
- How does an organization's compliance posture related to applicable laws, regulations, standards, contracts and policies change when business, and sometimes even customer and employee, information is stored in the clouds?
- How long does information put into the clouds stay in those clouds? Do the clouds have retention policies? Can information be permanently and completed removed from the clouds once it is put there?
- Are there any logs generated to show how that cloud information is accessed, copied, modified and otherwise used?
- Can all necessary information in clouds be easily retrieved during e-discovery activities? If so, what are the related costs involved?
- Are backup and recovery processes in place? Are they adequate for the organization's needs?
- What are the availability promises for the cloud service? Are they documented within a Service Level Agreement?
- What audit trails are generated and maintained for the organization's data?
- How quickly will the organization be able to obtain information about data access and associated logs?
- What laws, regulations, industry standards, contractual obligations, and organizational policies cover the data the organization is considering to have sent to the cloud?
- Does the cloud computing service have established and documented Information Security policies and supporting procedures?
- What do the cloud computing service's posted privacy and security policies say? Do they support its internal policies and contractual promises?

Encryption

Encryption is an effective method for any organization to use to help maintain information confidentiality and privacy. Numerous laws, regulations, industry standards, and growing numbers of contractual requirements require personal information and other types of confidential information to be encrypted.

For example, the Payment Card Industry (PCI) Data Security Standard (DSS) includes many directives to protect the wide range of business information from unauthorized disclosure. Just a couple of the specifics include "Requirement 4: Encrypt transmission of cardholder data across open, public networks" and "Requirement 7: Restrict access to cardholder data by business need to know."[55]

As another example, consider the new legal requirements for businesses to encrypt personal information. This trend is specifically to maintain the confidentiality of personal information and prevent identity theft and other related crimes. At least two states, Nevada and Massachusetts, have enacted laws requiring businesses to encrypt personal information, and more states are poised to follow suit.[56]

It is important to note and understand that the laws mandating encryption are applicable in addition to the at least 48 US breach notice laws currently in effect.[57] Breach notice laws provide the requirements that organizations must follow after a breach has occurred, but the new laws that include encryption requirements are aimed at preventing breaches from occurring in the first place.

Information Security and Privacy functional units need to work together to identify all the legal requirements for encryption, and then to identify the encryption solutions that will work best for their organization and business needs.

Certifications and trust seals

More businesses are placing trust seals on their web sites to show their customers that they have been validated as being trustworthy. According to a late 2008 US survey conducted by *Consumer Reports*, over 71% of online shoppers look specifically for third party seals to verify website security and privacy.[58]

---

55 Accessed November 2, 2009 from the PCI DSS documentation at https://www.pcisecuritystandards.org/.

56 *See* Nevada law, NRS 597.970, "Restrictions on transfer of personal information through electronic transmission, at http://www.leg.state.nv.us/NRs/NRS 597.html#NRS597Sec970.

See Massachusetts law, "201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth" at http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf.

57 Find a list of U.S. breach notice laws at http://www.privacyguidance.com/files/USStateandTerritoriesBreachNotificationLaws032209.pdf.and the list from law firm Perkins Coie at IVG.United States.C-7

58 "Which certifications are worth your time?" Accessed October 14, 2009 from http://ezinearticles.com/?Website-Verification-With-Third-Party-Seals&id=2115909

More businesses are also pursuing ISO/IEC 27001 certification to demonstrate to their business partners that they have good Information Security programs in place. As of August 8, 2009, 5,693 organizations (up from 3,530 total in June 2008 and up from the June 2006 total of 2,645) throughout the world had obtained such certifications, with the majority (3,191 organizations) located in Japan. The USA had only 94 (up from 48 in June 2008).[59]

More businesses are also relying upon SAS70 Type II audit reports[60] to certify business partner and vendor security, even though the scope of this report is not comprehensive and does not cover significant security issues. Additionally, it does not touch upon privacy practices at all.

Information Security and Privacy functional units need to work together to identify what, if any, trust seals, certifications or audit reports should be obtained to meet customer, investor and business partner expectations and to maintain trust.

Record retention and e-discovery

One of the AICPA/CICA Generally Accepted Privacy Practices (GAPP)[61], commonly used for auditing compliance with data protection laws worldwide, is that personal information should only be retained for as long as necessary to fulfill the stated purposes provided when the information was collected, unless a law or regulation specifically requires otherwise. This is a key exception, because of the many laws worldwide addressing how long many specific types of information must be retained. Here are just a few of the requirements within the U.S.:

- The Health Insurance Portability and Accountability Act-Requires that covered entities must not only ensure the security and appropriate access to health information while in transit through networks, but also ensure security while the information is in storage. Additionally, certain types of information related to access to protected health information must be maintained for six years from the date of its creation or six years from the date for which it was last in effect, whichever is later. Penalties include not only civil, but also potentially large fines and/or prison time.
- The Gramm-Leach-Bliley Act-Requires financial organizations with customers and consumers who are U.S. citizens to implement security to ensure the

59 Accessed August 8, 2009 from : http://www.iso27001certificates.com/

60 Statement on Auditing Standards No. 70 (SAS 70) is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) that provides the findings of an audit of a service organization's internal controls. There are two types of SAS 70 reports. A SAS 70 Type I report includes the auditor's opinion about the service organization's description of operational controls. A SAS 70 Type II eport includes the information contained in a Type I report in addition to the auditor's opinion on whether the specific controls were operating effectively during the audit period.

61 "Generally Accepted Privacy Principles." American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. 2009. Accessed November 1, 2009 from http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Generally+Accepted+Privacy+Principles.htm

privacy of non-public personally identifiable (NPPI) information, and must also establish formal Information Security programs governing the security and retention of NPPI. Both the organizations and individuals responsible for regulatory compliance within the organizations face potentially huge fines and/or prison time for non-compliance.

- The USA PATRIOT Act-Requires basically all U.S. organizations to record and report cash transactions of more than $10,000, or two or more related transactions involving more than $10,000, and certain transactions involving monetary instruments to Treasury's Financial Crimes Enforcement Network (FinCEN). The Act requires a program be established to prevent money laundering through the use of policies, procedures and internal access and security controls. Included in the requirements are specifications for record retention and safeguards, reporting, verifying customer identification, and responding to law enforcement requests. Additionally, money services businesses that have computerized data processing systems must integrate into their systems compliance procedures, such as record keeping and monitoring transactions, subject to reporting requirements. It specifies the government will have the right to review the electronic information upon its request within a reasonable timeframe. 5 years is given as the retention period for many of the records under the USA PATRIOT Act.
- The Securities Exchange Act Rules 17a-3 and 17a-4-Require that certain records must be preserved for either three or six years, depending upon the particular record.
- Internal Revenue Code Title 26 -Carries a penalty of up to $500,000 and three years in prison for destroying records. Records must be retained based upon the type of organization, but, in general, keeping records for at least 7 years to address this Code requirement is considered a good business practice.
- NASD Conduct Rules 3010 (Supervision) and 3110 (Books and records)-Include retention requirements. NASD 3010 requires that member firms establish and maintain a system to supervise the activities of each registered representative, including transactions and correspondence with the public. In addition, NASD 3110 requires that member firms implement a retention program, "Books and Records," for all correspondence involving registered representatives; it also requires the retention of customer records and transaction data in a reviewable format and in an easily accessible place.

Under the U.S. Federal Rules of Civil Procedure (FRCP), organizations must demonstrate that their electronic information is complete, accessible, and reliable. As a result, companies must formalize their retention management strategy and rapidly put in place the organizational and technological changes required to retrieve any given record.

In addition to these, there are a great variety of state and local level laws and regulations, and some of them have conflicting requirements. Legal requirements for retention is not unique to the U.S.; there are many other information retention laws worldwide. As just two examples:

- The directive for data retention in Bulgaria went in to effect on February 2, 2008. It requires Internet Service Providers and telecom companies to collect data from their clients and retain this data for 12 months.[62]
- The German data retention law entered into force on January 1, 2008.[63]

These and other evolving regulations require companies to comply with a tremendous number of retention periods, storage methods and other specifics, depending on a broad range of factors. These factors include which types of data the company collects, in which industries and which geographical regions the organization operates, and in which countries, states and local jurisdictions it operates.

Most organizations struggle with record retention issues, particularly for electronic records. Research by Gartner Group showed only 10 to 15 percent of organizations have applied some form of data retention strategy to their electronic records; all others have nothing, except most likely a data backup system.[64]

We cannot talk about retention without also considering e-discovery. According to the Enterprise Strategy Group, of 500 IT professionals surveyed in multiple industries, 50% of them were impacted by cases that required e-discovery, and 70% of those impacted had to retrieve email during the e-discovery process.[65]

Many organizations do not like to deal with e-discovery because it can be costly. According to e-discovery software vendor Attenex, when Lovells, the sixth largest international law firm in the world, had to determine the potential conspiracy and fraud claims involved in a complex multi-party transaction, it had to go through 35 gigabytes of data during the investigation stage. This would be comparable to going through two million pages of solid text. It also had to restore e-mail under tight staffing and cost controls. Using traditional electronic discovery methods, this took around one year to do and cost Lovells approximately $4-5 million.[66]

---

62 Accessed on December 26, 2009 from http://epic.org/privacy/intl/data_retention.html# implementation.

63 AccessedonDecember26,2009fromhttp://www.edri.org/edrigram/number6.1/germany-data-retentio

64 See "Electronic Records Management: Why Should Financial Executives Care?" by By Bill Lyons, Chairman and CEO, AXS-One; accessed November 1, 2009 from http://accounting.smartpros.com/x62877.xml

65 See "E-discovery rules double-edged sword for CIOs" by Linda Tucci, Senior News Writer. Accessed November 1, 2009 from http://searchdomino.techtarget.com/news/article/0,289142,sid4_gci1222185,00.html

66 Accessed November 11, 2009 from http://www.ftitechnology.com/casestudies/cost_reduction.aspx

The preponderance of electronic data has multiplied exponentially the records retention challenges within organizations. They can no longer keep track of paper documents to meet their regulatory and legal retention responsibilities; that day is long gone.

According to LogicaCMG[67], a small telecommunications company may generate 100 million records per day; storing these records for the maximum two-year period required under the EU Data Retention Directive would amount to about 72 billion records. The estimated cost of retaining that information varies from a couple of million Euros (US $1,351,613) to over 100 million Euros (US $135,161,308).

Information Security and Privacy areas must work together to create and oversee an effective lifecycle management program to mitigate information retention and e-discovery risk. A few important tasks include:

- Creating thoughtful, feasible, documented information retention and e-discovery policies and procedures.
- Maintaining documented retention schedules
- Performing periodic audits to ensure compliance with retention and e-discovery requirements
- Providing effective training about records retention policies, standards and procedures, along with ongoing awareness communications.

Information disposal

Many organizations spend significant time and money on activities and tools to prevent technology-based incidents (unauthorized network intrusions, malicious code, and so on). It seems, however, that controls are getting increasingly sloppy when it comes to controlling the disposal of old computer hardware and media, in addition to printed paper, all of which contain personal information.

The number of reports concerned with the disposal of personal information is increasing. Many Information Security and Privacy incidents have occurred through non-technical means by simply and thoughtlessly throwing away printed documents into publicly-accessible trash bins, or even putting computers, USB drives and sensitive documents out on the streets.

An interesting report published on October 18, 2007[68], written in conjunction with National Identity Fraud Prevention Week in the United Kingdom (UK), revealed that most businesses in the UK, and almost all their citizens, throw away documents containing personal information, such as account numbers, leaving them vulnerable to crime and fraud as a result of their not having been irreversibly

67 Accessed November 21, 2009 from http://www.mofo.com/news/updates/bulletins/12271.html

68 Accessed on November 1 2009 from http://www.sdbmagazine.com/news/news.asp?ID=7892.

destroyed, deleted or shredded prior to disposal. The rate of such risky disposal practices is up over 20% from the statistical findings originally issued in 2006.

Because of these alarming findings, a website, http://www.stop-idfraud.co.uk/, was created to educate individuals and businesses about the risks and how to better dispose of sensitive information. The site is interesting, with a variety of facts, statistics and recommendations. An especially important statistic is that, on average, "It takes 467 days to discover that you are a victim of identity fraud .according to Experian."[69] This points to the importance of organizations being very careful when making public statements, such as, "There is no evidence that personal information has been used for fraud" within even a few months following any kind of privacy breach, including when the breach was the result of improper disposal.

The U.S. has the Fair and Accurate Credit Transactions Act (FACTA) Disposal Rule[70] plus several other laws that include requirements for safeguards for proper disposal of personal information. According to the U.S. Federal Trade Commission (FTC), the FACTA Disposal Rule "applies to people and both large and small organizations that use consumer reports, including: consumer reporting companies; lenders; insurers; employers; landlords; government agencies; mortgage brokers; car dealers; attorneys; private investigators; debt collectors; individuals who pull consumer reports on prospective home employees, such as nannies or contractors; and entities that maintain information in consumer reports as part of their role as a service provider to other organizations covered by the Rule."[71]

The provisions of the FACTA Disposal Rule require proper disposal of consumer information, and apply not only to credit reports, but also to any type of media containing the information contained within credit reports. The FTC reported that when it comes to the proper disposal of information in consumer reports and records, organizations need to demonstrate due diligence to protect against "unauthorized access to or use of the information." The FTC Disposal Rule enables companies to consider the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology before deciding, and documenting, what measures are reasonable.

FACTA is not the only rule requiring proper disposal of personal information. The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and Privacy Rule also require the proper disposal of personal information. In addition to these regulations, there are a wide range of U.S. state-level laws that have personal information disposal requirements. Federal bank and credit union regulators, along with the Securities and Exchange Commission (SEC), have finalized their own disposal

69 Accessed November 15, 2009 from http://www.realtime-itcompliance.com/information_security/2008/05/business_leader_primer_for_eff.htm

70 *g* Disposal Rule at ftc.gov/os/2004/11/041118disposalfrn.pdf.

71 Accessed November 1, 2009 from http://www.ftc.gov/opa/2005/06/disposal.shtm

rules under Section 216 of FACTA, which are similar to the FACTA Disposal Rule, however, the FACTA rule covers a much wider range of industries and organizations than any previous regulation. It effectively covers any type of business that collects, handles or processes information that is considered to be consumer information.[72] In fact, many companies may not even be aware that FACTA applies to them. The National Association for Information Destruction (NAID)[73] estimates there are over 10,000 U.S. businesses that fall under the Disposal Rule. Considering the FTC's description of the organizations to which the rule applies, it is probably much higher than this.

It is important to realize that the FTC has stated that similar protective measures should be taken by those who dispose of any records containing a consumer's personal or financial information, whether or not they are bound by the Disposal Rule.

Similar disposal rules are also found, and are emerging, in other countries. For example, the UK has the Data Protection Act that requires, among other safeguards, that confidential information must be securely disposed of. The British Standard for the secure destruction of confidential material, BS 8470:2006[74], applies to confidential information in all its forms and supports compliance with the Data Protection Act. It requires companies to dispose of confidential information by shredding or using disintegration. Confidential materials include such things as paper records, computer hard drives, CDs/DVDs and even company uniforms.

The multiple regulations and laws, in addition to recent personal information breach incidents, should serve as a wake-up call to organizations to ensure they have appropriate policies and procedures in place to properly dispose of personal information when it is no longer needed. Not only do businesses risk large fines and penalties from noncompliance with applicable regulations, but they also risk what is likely even greater organizational impact from lost consumer confidence and the bad publicity that could result from just one personal information disposal incident.

The Information Security and Privacy functional units should collaborate to most effectively address the issue of information disposal by:

- Creating a documented, fully implemented, auditable and executive-supported disposal program.

72 Any information an individual gives an organization to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application). See more explanation at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus67.pdf

73 NAID is a U.S. based organization comprised of around 1,200 data destruction vendors.

74 See "BS 8470:2006 Secure destruction of confidential material. Code of practice." at http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030127562

- Providing effective awareness communications and ongoing training to your personnel and business partners about the proper way to dispose of information.

Cyber risk insurance

It has been well established throughout this chapter that cyber risks are increasing, along with privacy breaches. All risks do not come from outsiders. A November 2009 report shows that 48% of workers in the UK will steal data if fired, and that customer personal information was the most likely target of such theft.[75] Add to malicious attempts to steal data the huge numbers of Information Security incidents and Privacy breaches that occur as a result of mistakes and lack of awareness. Business leaders are often desperate to try to mitigate their losses from these likely breaches.

Due to the increased risks relating to identify theft and breach notification requirements and costs business leaders are also increasingly seeking to purchase cyber risk insurance. According to the 2008 CSI/FBI Computer Crime and Security Survey[76], 34% of U.S. companies indicated that their organizations use cyber insurance. This number has risen from 29% in the 2007 survey[77].

What risks are organizations trying to mitigate by purchasing cyber risk insurance?

- Loss or damage to data
- Loss of computer resources
- Legal liability to others
- Loss or damage of reputation
- Loss of market capitalization

The Risk Management or Finance functional units typically lead the cyber risk insurance application and quote process, however, the insurance application will typically require the organization to complete a risk assessment questionnaire of the organization's environment. In addition, most cyber risk insurers will conduct a more extensive security assessment, often from an outsourced organization, to determine the organization's insurability. These assessments are typically based on the ISO/IEC 27001 and ISO/IEC 27002 standards[78]. Information Security and

75 "Stealing company data? It is just an insurance policy." ComputerworldUK. Accessed November 25, 2009 from http://www.computerworlduk.com/management/security/data-control/news/index.cfm?newsid=17733

76 "Computer Crime and Security Survey 2008." The Computer Security Institute. 2008?. Accessed November 3, 2009 from http://i.zdnet.com/blogs/csisurvey2008.pdf

77 "Computer Crime and Security Survey 2007," The Computer Security Institute., 2007. Accessed November 3, 2009 from http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

78 ISO 27001 and ISO 27002 Information Security Standards see http://www.27000.org/

Privacy leaders must be involved, and work together, to ensure the assessments are answered completely and accurately.

Employee monitoring and checks

The significant insider threat is making organizations much more cautious in their hiring decisions. The turbulent economic times increase the worries that someone will be hired who will do bad things, like steal customer or employee information, or commit fraud, once they are on the payroll. The types of background checks and ongoing employee screening are increasing. In late 2009, the top trends in screening job candidates included[79]:

- More organizations in multiple countries are using automated databases that provide quick access to information for doing background checks. (A related issue to consider with this activity is the transmission of data across country borders, which is not allowed in many situations.)[80]
- More job applicants worldwide are providing false information about why they are applying for jobs. With record levels of unemployment, mass layoffs and the foreclosure crisis continuing, people looking for jobs are getting increasingly desperate. This is leading to many people losing their moral compass, resulting in an increase in the use of fake credentials, degrees, references and exaggeration of work experience. Industry reports of misrepresentation of information range from 40 to 60% of applicants misstating information on their resume. There are over 3,000 diploma mills worldwide making a lot of money selling fake degrees, references and credentials, which requires organizations to remain more diligent than ever in checking applicant information. Despite pressures to reduce expenses, HR Managers are more often checking backgrounds and references to help prevent hiring unqualified candidates and people who are focused on depleting company resources through fraud, identity theft, and other types of criminal activities.
- With the continuing threat of identity theft, employee fraud and theft more firms are using infinity screening (also referred to as re-occurring and post hire screening)[81] as a way to combat this problem. Additionally, as just noted, fake credentials are readily available, so employers must continue to verify the legitimacy of degrees and credentials earned by current employees.
- HR executives are, once again, emphasizing the use of old-fashioned reference checks. When these checks are done correctly, they provide valuable information and help to prevent bad hiring decisions.

---

79 From "Seven Trends in Background Screening That will Impact Talent Acquisition and Hiring." September 11, 2009. Accessed on November 13, 2009 from http://www.onrec.com/newsstories/25963.asp.

80 Many countries do not allow the transmission of personal information across borders to a country that is considered to have unacceptable privacy protections. For example, the EU does not consider the U.S. to have acceptable privacy protections.

81 These are checks that occur with active employees,

- There are increasing numbers of legal challenges to the growing practice of using credit checks in the hiring process. For example, Washington Stateand Connecticut have laws that prohibit the use of credit checks in the hiring decision,[82] and it is likely more states will follow suit.

The concerns about hiring dishonest individuals and criminals have led to some bad screening practices by some organizations. As just one of many possible examples, during the first half of 2009, a Bozeman, Montana city government agency actually required job applicants to provide their IDs and passwords for any online social networking type of site in which they participated[83].

Bozeman's concern about hiring someone who may be doing unsavory things online is understandable, however, asking each applicant to share user IDs and passwords is not only a huge privacy problem, it is also a violation of standard and internationally-accepted Information Security practices to never share IDs and passwords with anyone. This would be similar to employers asking job applicants for the keys to the applicants' homes and cars so the employers can go through them and peek in every nook and corner to see if there is anything around about which they disapprove.

There are also demonstrably understandable reasons why organizations are engaging in more activities to monitor the online activities of employees. Consider the following:

- **December 2008**: Photos of three teen girls posing in their underwear taking baths in the large sinks at the northern California KFC where they worked were posted on MySpace and soon went viral, doing some significant public relations damage to the restaurant chain.[84]
- **February 2009**: Someone from a Wisconsin medical center made an anonymous call to the sheriff to report a nurse had taken photos of a patient with her cell phone and posted the photos to her Facebook page.[85] Investigation revealed two nurses actually each took a photo of an x-ray of a patient who was admitted to the emergency room with "an object lodged in his rectum." The two nurses who took the photos were fired. The medical center had its reputation badly smudged.
- **June 16, 2009**: A New Jersey federal jury ruled that the managers of a Houston's restaurant in New Jersey violated the Stored Communications Act

82 See http://www.hrscreener.com/current_issue/index.asp?id=1161

83 "Bozeman City job requirement raises privacy concerns," Montana's News Station. Accessed November 21, 2009 from http://www.montanasnewsstation.com/Global/story.asp?S=10551414&nav=menu227_3.

84 Accessed June 2, 2009 from http://www.dailymail.co.uk/news/worldnews/article-1094130/Bargain-bath-Three-KFC-workers-fired-bathing-bikinis-restaurant-sink-putting-photos-internet.html

85 Accessed August 5, 2009 from http://www.fiercehealthcare.com/story/wi-nurses-fired-over-cell-photos-x-ray/2009-02-27.

and the New Jersey Wire Tapping & Electronic Surveillance Act by intentionally accessing a MySpace page that employees used without authorization, and then firing two employees for derogatory remarks about the management made to the group[86]. The restaurant was ordered to pay compensatory and punitive damages for maliciously and without authorization invading a password-protected, invitation-only employee gripe group on MySpace.

To address the risks of employees doing things online that could negatively impact an organization, the Information Security, Privacy, HR and legal areas need to work together to:

1. Have policies in place that clearly list unacceptable online activities, as applicable for the organization, such as:

   a) Personnel must not post client, co-worker or business information or personal information on social networking sites or through other Web 2.0 technologies

   b) Personnel must not post the organization's logo, trademark, etc. on social networking sites or through other Web 2.0 technologies, and so on.

2. Establish documented procedures, performed by persons with these responsibilities within their job descriptions, to monitor the Internet for mission critical and confidential information that may possibly be leaked.

3. Establish safeguards and controls to keep sensitive information from leaving the organization's network, and to monitor when such attempts are made.

4. Provide regular training and ongoing awareness communications about the threats, vulnerabilities, and resulting risks of using Web 2.0 technologies and sites, and the reasons why personnel need to be concerned and take precautions, not only to protect the business, but also to protect themselves, families and friends.

Data inventories and data flows

Businesses, of all sizes and in all industries, possess a staggeringly large amount of personal information. But is all this information being appropriately protected? Is the confidential and personal information being protected? Do the organizations even know all the locations where personal information is collected, stored and accessed?

It is more important than ever before for organizations to be able answer the following:

- Under which circumstances and representations was the personal information collected?
- How is personal information being used?

86 Accessed November 3, 2009 from http://www.martindale.com/communications-law/article_Ogletree-Deakins-Nash-Smoak-Stewart-PC_820280.htm.

- With whom is personal information being shared?
- How and where is personal information being stored?
- Who has access, authorized or not, to personal information?

Unfortunately, many, if not most, businesses do not know the answers to these questions.

The key to controlling and safeguarding personal information is knowing where it is and how it is used. These simply stated, but complex to accomplish, concepts are the basis for most existing consumer Data Protection and Privacy laws. Organizations must maintain an information inventory to be able to effectively protect information. An organization cannot claim that information is secure if its personnel do not even know where and how it is being used.

Organizations must know where sensitive data is located, how it is used, how it is shared, how it is accessed, how it is secured and how it is destroyed. The ease in establishing the inventory depends upon the organization's maturity level in data management, change management and exception management documentation.

The Privacy and Information Security areas require these areas to work together for:

- Identifying information that is considered to be personal information.
- Maintaining an inventory of personal information storage locations

Business resiliency and pandemic planning

When establishing business resiliency plans, it is important to include input from the Information Security and Privacy units. Consider some of the common aspects of disaster recovery and business resiliency and the related data protection issues associated with each that information security and privacy areas can collaborate on to be most effective[87].

1. Controlling access during network recovery. An objective of disaster recovery is to minimize risk to the organization during recovery. This includes minimizing the risk to privacy. There should be a baseline set of documented access controls[88] to use during recovery activities to prevent intrusions and privacy breaches during the recovery period.

2. Controlling access to mobile computers. Mobile computers are increasingly used for regular business activities. During a disaster or business disruption of any type, they are used even more. Businesses often allow employee-owned

87 This section is an updated version of Rebecca Herold, "Converging Information Security and Privacy Activities During Business Continuity," Disaster Recovery Journal, October, 2009.

88 For example, documentation should exist that shows the allowable requirements to establish during network recovery, typically for the IDs and positions that have network and systems administrative capabilities, and the positions that have the authority to approve of resource access authorizations.

computers to be used. The increased use of these mobile devices during such times should not put information and privacy at unnecessary risk.

3. Controlling facilities and physical access. One of the most effective means for limiting the damage from a malicious act, which could potentially result in a privacy breach, is to limit physical access to the recovery data center and its edges, including the floors above and below the data center and the adjacent areas.

Controlling access to backup media. Backup media can contain massive amounts of PII. For example, on February 27, 2008, the Bank of New York (BNY) Mellon lost six to 10 unencrypted tapes while it was transferring back-up tapes that contained names, addresses, birth dates and Social Security numbers of over 12.5 million of their customers. The bank is still paying for that incident as more civil suits continue to be reported[89].

4. Limiting public conversations about personally identifiable information (PII). During disaster recovery many businesses not only need to perform work in *ad hoc* work locations, but they also spend much of their waking time discussing with colleagues the details of the recovery. Often these discussions happen over lunch, dinner or coffee at a nearby café, through cell phone discussions while traveling in airports, or while also trying to run personal errands such as buying groceries, taking children to school events and doing other activities in public spaces.

5. Making others custodians of PII. Oftentimes third parties are contracted to assist with recovery and continuity processes. Backup media is often stored within a vendor site specializing in such services. Companies often contract with vendors to use their cold or hot sites[90] for recovery. Some businesses have arranged with other companies to use a portion of their computer facilities during recovery. Information is often shared with government and law enforcement after a disaster.

Business resiliency issues and situations that require the involvement of both the Privacy and Information Security functional units require these areas to work together for:

- Documenting appropriate access controls for personal information during recovery and continuity activities
- Documenting the personal information items that can and cannot be stored on mobile computers and electronic storage devices

89 For more discussion of this see, "Suspected Citi breach is an old bank problem" dated December 22, 2009 at http://www.marketwatch.com/story/an-old-breach-still-bothers-banks-2009-12-22.

90 A "cold site" is a facility which can be used to house data processing facilities in the event of a disaster. A cold site typically contains the appropriate electrical and heating/air conditioning systems, but does not contain equipment or active communication links. Cold sites are longer to get up and running than hot sites, but they are much less expensive than hot sites.

A "hot site" is a facility fully equipped to take over data processing operations upon short notice. A hot site contains fully configured equipment and communications links. Hot Sites provide a very high level of disaster recovery protection, but the cost of maintaining a hot site facility can be extremely high.

- Documenting personal information access and security controls to use during business resiliency activities
- Identify the locations of equipment containing personal information
- Identify the locations of repositories of printed personal information
- Establish physical access control requirements for the equipment and print repositories during business resiliency activities[91].
- Determining if installing surveillance, such as closed circuit television, is appropriate for these areas to minimize security and privacy risks
- Establishing policies and procedures to secure personal information on backups, including encryption and access controls.
- Documenting how to effectively make personal information backups for not only central repositories, but also endpoints.
- Documenting when and how often to take backups off-site.
- Documenting how to effectively secure personal information backups at off-site locations.
- Including privacy and security issues, such as public meetings and computer access, within disaster recovery and business continuity training.
- Providing regular and ongoing awareness communications about not discussing personal information in public, along with any of the many examples of how such actions have resulted in privacy breaches.
- Identifying and documenting all third parties contracted to help with business resiliency activities.
- Ensuring that appropriate security and privacy requirements are included within the contracts.
- Implementing policies and procedures to involve Information Security and Privacy units when law enforcement and other investigators want access to personal information to ensure such information sharing is appropriate, and that necessary controls are established prior to sharing.

Policies and procedures

Consider all the many types of policies and procedures that exist within an organization. Documented policies and procedures are necessary for consistency and to ensure that personnel clearly understand what is expected of them while they are performing their daily job responsibilities.

Privacy and Information Security practitioners share responsibilities for many of these policies; however, they should not each create a separate policy to address

91 "Business resiliency" generally is the term used to describe the ability to keep business activities running even under adverse conditions of any type.

the same topics. The author has done research for companies to analyze their complete assortment of policies, and she has found many of the same topics having different treatment in different policies existing within the Information Security area, Privacy area, HR area, and physical security area, just to name a few. When there are multiple policies for the same topic, it destroys the effectiveness of all the policies; employees do not have a clear directive for the topic, but instead seem to be given a choice of which policy to follow. This applies to both privacy and public sector policies, which are generally similar in form and function.

The existence of formally documented policies has also been a major factor in court cases when applying the U.S. sentencing guidelines[92]. Issues under the U.S. Federal Sentencing Guidelines that impact the severity of the judgments include consideration of the following:

- How frequently and how well does the organization communicate its policies to personnel?
- Are personnel effectively getting trained and receiving awareness?
- What methods does the organization use for such communications?
- Does the organization verify that the desired results from training occur?
- Does the organization update the education program to improve communications, and to get the right message out to personnel?
- Does the training cover ethical work practices?
- Is there an ongoing compliance and ethics dialogue between staff and management?
- Is the management getting the same educational messages as the staff?

The need for policies and procedures also creates challenges in most businesses, resulting in:

- Duplication of effort
- Gaps in effort
- Turf wars

92 According to the Department of Justice, in 1995, 111 organizational defendants were sentenced according to the Guidelines, with 83 cases receiving associated fines. By 2001, the number of organizational defendants sentenced rose to 238, with 137 receiving fines and 49 receiving a fine as well as ordered to provide restitution.

Average fine: $2.2 million

Average restitution awarded: $3.3 million 90 of those sentenced had no compliance program

The numbers of fines and penalties are now increasing with the implementation of the updated Guidelines, which went into effect in November.2007

- Misunderstanding
- Inconsistency

Information Security and Privacy areas units work together to address these challenges.

Systems and Applications Development

Alarmingly large numbers of Information Security incidents and privacy breaches continue to occur as a result of poorly engineered systems and applications that leave them vulnerable to exploitation. Consider the following incidents, all of which were reported in November 2009:

- Notre Dame University in South Bend, Indiana reported that an error in an application resulted in having the "personal information of some past and current employees -including name, social security number and birth date" posted onto a public website.[93]
- A report containing the personal information, including Social Security numbers, about 4,500 present and past students at Chaminade University was posted on the school's public Internet web site.[94]
- The Social Security numbers, home addresses and phone contacts for 300 -355 students who applied for admission to Cal Poly Pomona in the past six years were posted online in a publicly accessible location because of faulty applications change management procedures. "Google and other search-engine companies mined the data."[95]

It is likely that these privacy breaches would not have occurred if Information Security and Privacy had been appropriately addressed when the applications and systems were created.

Security and privacy must be built into every application and system from the very start of the development lifecycle and continue to be addressed until the application or system is retired. Creating applications and systems that appropriately address Information Security and Privacy risks and compliance requirements does not happen by accident. Information Security and Privacy compliance and risks also cannot be effectively addressed by waiting to the end of the development phase, but this is what happens in many organizations. Effective Information Security and Privacy objectives are accomplished only when every designer, developer,

---

93 "Notre Dame security breach potentially affects employees." WNDU TV. November 20, 2009. Accessed November 30, 2009 from http://www.wndu.com/localnews/headlines/70674717.html

94 "Student data posted in error." November 7, 2009. Honolulu Advertiser. Accessed November 20, 2009 from http://www.honoluluadvertiser.com/article/20091107/NEWS07/911070324/Student+data+posted+in+error.

95 "Personal data of Cal Poly Pomona applicants inadvertently put online." Los Angeles Times. November 13, 2009. Accessed November 30, 2009 from http://latimesblogs.latimes.com/lanow/2009/11/personal-data-of-cal-poly-pomona-applicants-inadvertently-put-online.html.

tester and manager working on the project addresses the risks on a continuing basis throughout the entire development lifecycle.

It is important for business leaders throughout the enterprise to understand the system development life cycle (SDLC)[96] and how decisions made can impact, negatively or positively, the entire business. First and foremost, systems and applications must be built to support the business in the most efficient and effective manner possible. Business leaders must be involved with the process to ensure systems and applications are being developed to meet this goal; the Information Technology (IT) units cannot create applications and systems on their own and reach this goal. Second, applications and systems must be created to reduce risk to the level acceptable by the business as well as to attain compliance with applicable laws, regulations, and contractual requirements.

Organizations must ensure that Information Security and Privacy are constructed throughout the SDLC:

- To ensure that systems and applications support corporate policies and procedures
- To protect data throughout the entire information life cycle
- To meet requirements in data protection laws and regulations requiring information protection, such as access controls, access logging, availability, and so on

Organizations must follow a well-defined SDLC process to address Information Security and Privacy every step of the way through the use of policies, procedures, standards, privacy impact assessments (PIAs)[97], and Information Security risk assessments. The objective of incorporating Information Security and Privacy is not to totally overhaul an existing SDLC project management process, but to add well-defined security and privacy checkpoints and security and privacy deliverables. The ultimate goal is to make the applications and systems as secure as reasonable based upon risk and to ensure compliance with applicable data protection laws.

There are many Information Security and Privacy checks that should be made within each of the lifecycle phases. Information Security and Privacy units must work together to ensure appropriate checks are made during each of these phases. Some important collaboration points include, but are not limited to, the following:

- Not to wait until an application or system is already in production to make it secure and address privacy; this is too late to ensure effective security and privacy. Such a band-aid approach is dangerous to the business.

---

96 The "Systems Development Life Cycle," along with the Software Development Life Cycle, are terms commonly used in systems engineering and software engineering to describe the process of creating or altering computer systems and programs, and the models and methodologies that people use to develop these systems and programs.

97 For more information about PIAs see "PIAs Provide Privacy Purview" by Rebecca Herold at http://www.privacyguidance.com/etechnology_articles.html.

- Effective security and privacy practices need to be incorporated into all the applications and systems layers involved, such as the network, host, application, storage, end-points, and other applications and systems components.
- It is important to ensure that clearly written and easily accessible information security and privacy policies, standards, and guidelines are used as frameworks for the security and privacy being constructed within each application or system.
- To implement, or follow, the existing, policy deviation-exception process[98].
- Create checklists that include step-by-step instructions within every SDLC phase for Information Security and Privacy.
- Personnel training is crucial to the success of incorporating security and privacy into each relevant application or system; organizations should make sure it occurs not just once, but on an ongoing basis during the life of the application or system.

Information Security and Privacy are ongoing and always changing processes; someone should be for addressing these issues during the lifetime of the application or system.

Conclusion: Information Security and Privacy collaboration improves business

All organizations benefit from taking a practical, structured, approach for integrating privacy and security responsibilities and activities throughout the enterprise. Not only will the security program be stronger, but there will also be more comprehensive and risk-based compliance for Data Protection and Privacy laws. Organizations of all types, in both the private and public sectors, need to take at least five important steps to achieve successful collaboration:

Step 1: Identify business overlaps

Identify the business issues for which Information Security and Privacy activities and responsibilities overlap. Whenever personal information is collected, handled, transmitted or stored, there will be overlapping issues.

Step 2: Determine risks

Determine the privacy and security risks for the overlapping issues. As just one of many potential examples, spyware is a shared concern. The Information Security unit must identify the many ways by which spyware can make its way into the organization, such as from Internet web sites, personnel using peer-to-peer tools such as instant messaging (IM) and texting, and via email attachments, just to name a few. Privacy leaders must know the types of personal information vulnerable to

98 A centralized department or position should be the only area authorized to make policy exceptions to ensure that the exceptions are 1) actually necessary, 2) tracked, and 3) allowed for only a limited period of time as necessary for the purpose of the exception.

being captured through spyware, and address the related regulatory requirements that require personal information protection from this type of risk.

Step 3: Establish policies and procedures

The privacy and security areas must work together to establish feasible, effective policies to address the identified risks. If these areas do not work together, there will be coverage gaps and multiple conflicting policies from different areas of the organization covering the same topic.

The author recently did a policy analysis for a large multi-national organization, covering all the twelve departments that issued policies throughout the organization. I found multiple gaps, as well as thirty-eight Information Security and Privacy issues that were covered by more than one policy, resulting in conflicting directives from different departments within the organization. Many policies were worded in a way that created a conflict between the policies. For example, the human resources (HR) policy for mobile workers did not require the business information to be encrypted on their computers, but the Information Security mobile workers policy had an encryption requirement.

Having different policies for the same topic, maintained by more than one department of the company, creates the risk that personnel will choose to follow the policy that is most convenient for their needs, and then claim they were in compliance with the corporate policy if they are found to be in noncompliance with the policy maintained by a different area. There should be only one policy per issue to make each policy effective and remove the subjective compliance choices that exist with multiple policies.

The Privacy and Information Security units must also collaborate, and work in partnership with, each business unit, to ensure that documented procedures are created to support the policies.

Step 4: Integrate security and privacy into the business culture

Organizations will have ineffective Information Security and fail to meet privacy requirements and expectations if they do not make Information Security and Privacy part of everyday work. Three effective ways to start creating this pervasive security and privacy culture and integrate into everyday job activities include:

- Document security and privacy responsibilities into job descriptions. This will help to ensure that personnel understand that addressing privacy and safeguarding information is not a stand-alone operation or someone else's responsibility; it becomes a responsibility within each person's job duties.
- Include security and privacy within job appraisals. When personnel know that the annual appraisal considers how securely they perform their job responsibilities and how well they protect personal information, they will be more diligent in keeping confidential papers locked away, keeping their computers locked when they are not at their desks, and thinking twice before sending personal information in email messages or loading it onto mobile computers and storage devices.

- Include privacy and security considerations into daily procedures. Organizations should incorporate privacy and security checks into all procedures that involve handling or accessing personal information.

Step 5: Implement cooperative awareness and training

Organizations will experience fewer incidents when the Privacy and Information Security units work together to implement cooperative awareness and training and integrate them throughout the enterprise. Well-informed personnel not only have the knowledge to protect personal information; training also makes them more accountable for their actions.

Organizations will be able to assess the improvement that a thoughtful, integrated information security and privacy program has by:

1. Establishing benchmarks. Before launching training awareness activities, they should measure security and privacy awareness within the organization.

2. Developing targeted training applicable to job roles. Provide general training to all personnel, in addition to providing customized, targeted training to units that have significant responsibilities involving personal information. These areas include, but are not limited to, call centers, marketing, IT, and HR.

3. Providing ongoing awareness communications and activities. Training must be complemented with ongoing awareness communications to reinforce security and privacy requirements, and to keep these issues in employees' minds while they perform their day-to-day work.

4. Evaluating how well awareness has been raised. Following training events and awareness activities, organizations should evaluate how much personnel knowledge has increased, as well as identify where improvements and more effort still need to be made.

It is critical for organizations to address Information Security, Privacy and compliance issues in a thoughtful and collaborative manner throughout the organization. It is critical for those responsible for Information Security to work closely and in partnership with those responsible for Privacy and the associated legal and compliance requirements and issues. Lack of this convergence will leave privacy and security gaps within businesses and government agencies, creating vulnerabilities waiting to be exploited. Lack of convergence will also result in having multiple areas putting out conflicting directives for the same business topics. It is also critical for personnel to have the knowledge to use information resources securely and in a way to protect privacy.

Successful programs require Information Security, Privacy, compliance, legal and IT units and their associated strategies to be complementary and integrated throughout all of the enterprise, within every business process and at every level within the organization. When Information Security and Privacy units in all types of organizations work together and collaborate, there are fewer incidents, less negative business impact, and business is improved.