

---

---

# **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<sup>®</sup>**  
NEW YORK

**OXFORD**  
UNIVERSITY PRESS

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

Copyright © 2010 by Oxford University Press, Inc.  
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.

All rights reserved. No part of this publication may be reproduced, stored in a  
retrieval system, or transmitted, in any form or by any means, electronic,  
mechanical, photocopying, recording, or otherwise, without the prior  
permission 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

#### **Note to Readers:**

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is based upon sources believed to be accurate and reliable and is intended to be current as of the time it was written. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought. Also, to confirm that the information has not been affected or changed by recent developments, traditional legal research techniques should be used, including checking primary sources where appropriate.

*(Based on the Declaration of Principles jointly adopted by a Committee of the  
American Bar Association and a Committee of Publishers and Associations.)*

**You may order this or any other Oxford University Press publication  
by visiting the Oxford University Press website at [www.oup.com](http://www.oup.com)**

## 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,”<sup>®</sup> 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](mailto: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)<sup>1</sup> 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)<sup>2</sup>, 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<sup>3</sup> 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<sup>4</sup> security administrator.<sup>5</sup> 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<sup>6</sup> 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/adminsimpleregtext.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](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](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/eleagal\\_regulations.html](http://www.privacyguidance.com/eleagal_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.<sup>7</sup> 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

---

<sup>7</sup> 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<sup>8</sup>**

**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<sup>9</sup>**

**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<sup>10</sup>**

- 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](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/USStateTerritoriesBreachNotificalawsasof07.20.09.pdf>  
Many assorted state and territory credit freeze, medical privacy, and other privacy-impacting laws see [http://www.privacyguidance.com/elegal\\_regulations.html](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](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<sup>11</sup>**

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.<sup>12</sup> 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<sup>13</sup> 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](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®)<sup>14</sup> 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<sup>15</sup>
- COBIT<sup>16</sup> 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<sup>17</sup>
- OECD/GAPP principles are being used to address privacy risks<sup>18</sup>

**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<sup>19</sup>. 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<sup>20</sup>, 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](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<sup>21</sup>, 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<sup>22</sup>. 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<sup>23</sup> 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](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<sup>24</sup>**

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<sup>25</sup>**

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/USStateTerritoriesBreachNoticeLawsasof07.20.09.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<sup>26</sup>
- Hong Kong: Hong Kong: Code of Practice on Consumer Credit Data (2003)<sup>27</sup>
- India: Information Technology Act, 2000 (as amended by Information Technology Act, 2008)<sup>28</sup>
- Ireland: Data Protection Commissioner Breach Notification Guidance<sup>29</sup>
- Germany: *Bundesdatenschutzgesetz* (Federal Data Protection Act, “BDSG” or the “Act”)<sup>30</sup>
- Canada: Office of the Saskatchewan Information and Privacy Commissioner Privacy Breach Guidelines<sup>31</sup>

**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](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/CCDCCode\\_eng.pdf](http://www.pcpd.org.hk/english/files/ordinance/CCDCCode_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](http://www.oipc.sk.ca/Resources/Privacy%20Breach%20Guidelines1%20(3).pdf)

































































