

A practical guide for operational information security and privacy convergence

 Jan 1, 2009  Save This

The Privacy Advisor | A practical guide for operational information security and privacy convergence 
by Rebecca Herold, CFI, CIPP, CISO, CISSP, CISM, CISA, ILM

"Privacy requires the implementation of information security controls and appropriate safeguards."

The need for convergence is nothing new

With all the recent talk regarding a convergence of information security and privacy it bears noting that this is not a new idea. Such convergence has actually existed ever since privacy became a concern. After all, privacy requires the implementation of information security controls and appropriate safeguards.

I experienced this relationship firsthand during the early 1990s before the passage of the Gramm Leach Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA). At the time, although bills addressing privacy had been considered in the U.S. and around the world, the Organisation for Economic Co-operation and Development (OECD) Privacy principles were the basis for most of the privacy requirements. While establishing the security requirements for one of the very first online banks, I recognized the need for a privacy policy based not upon legislation but on the need to obtain and maintain customer trust. This policy, based predominately upon the OECD Privacy principles, brought the need for security controls clearly into focus.

Convergence issues

Over time, I've identified 20 business areas where information security and privacy responsibilities and activities converge—a number that grows as technology, laws and business evolve. Understanding and complying with the multiple requirements of the 45 U.S. privacy breach notice laws is a recent example of how privacy and information security need to work together for effective management enterprise-wide.

Additionally, the growing number of incidents, accompanied by growing numbers of fines, penalties and civil actions, emphasize the need for convergence. The basics on complying with the hundreds of laws and regulations involves:



- knowing the information that is considered personally identifiable information (PII) within the organization;
- knowing where this PII is collected, stored, and leaves the organization; and,
- establishing effective safeguards to protect this PII throughout the entire information lifecycle.

Privacy is not strictly a legal issue, and information security is certainly not strictly a technical issue; privacy and security intersect in many ways.

Unequal authority in the organization

Unfortunately, responsibilities for privacy and information security often fall within different areas of an organization, and often at different levels within the organizational structure. I have seen firsthand how poor communication and unequal authority among these groups can lead to either gaps in privacy protections or conflicting directives on the same issue.

For example, a few years ago a large manufacturing organization created the privacy responsibility within its law office with a direct reporting responsibility to the CEO. The information security responsibility, on the other hand, was many levels down in the organization. The information security officer (ISO) was a manager, reporting to a director, reporting to a CIO, reporting to the operations VP, reporting to the CEO. The ISO was worried about the proliferation of laptops used for business processing, particularly for processing the orders of individuals as well as other companies. She did a risk assessment and submitted the resulting report with a recommendation to require full-disk encryption on the laptops.

The recommendation was denied because, according to the opinion rendered by the privacy officer in the law office, no laws explicitly required encryption, and the expense to implement encryption would not be necessary to advance the business. There had been no discussion between the privacy officer and the ISO prior to issuing this opinion. In this example, the decision was made purely on the letter of the law.

Information security risks were not considered even though most data protection laws require consideration of risks to be the basis for security decisions.

A thorough understanding of information security risks is required before adequate and proper safeguards can be implemented to meet risk-based compliance requirements. Close collaboration and mutual respect between functional areas will ensure effectiveness in the respective information security and privacy programs.

Integrating enterprise privacy and information security

Organizations will benefit from taking a practical, structured approach for integrating privacy and information security responsibilities and activities enterprise-wide. 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.

Step 1: Identify business overlaps

Identify the business issues where information security and privacy activities and responsibilities overlap. Wherever PII is collected, handled, transmitted or stored, there will be overlapping issues. You should find at least 20 overlaps (and maybe more).



Step 2: Determine risks

Determine the privacy and information security risks for the overlapping issues. Spyware, for example, is a shared concern. Information security should identify ways in which spyware can make its way into your organization (e.g. Internet Web sites, personnel using peer-to-peer tools such as instant messaging and texting, e-mail attachments, etc.). Privacy should identify the types of PII vulnerable to spyware, and address the related regulatory requirements that require PII protection from this type of risk.

Step 3: Establish policies and procedures

The areas must work together to establish feasible, effective policies to address the identified risks. If this doesn't happen, there will be coverage gaps and multiple conflicting policies on the same topic.

Recently I conducted a policy analysis that included 12 departments of a large multinational organization. I uncovered 38 information security and privacy topics covered by multiple policies, as well as numerous gaps. Many policies were worded in a way that created conflict and confusion. In addition, there were conflicting directives from different organizations. For example, the HR policy for remote workers did not require encrypting business information, but the information security policy had an encryption requirement for remote workers.

Having different policies for the same topic, maintained by more than one department, creates the risk that personnel will choose to follow the policy that is most convenient for their needs, and then claim compliance with corporate policy if found to be in non-compliance with any other departmental policy. There should be only one policy per topic to ensure policy effectiveness and eliminate staff choice and confusion.

The privacy and information security areas must also collaborate and work with all business units to ensure that documented procedures are created to support policies.

Step 4: Integrate information security and privacy into the business culture

Unless information security and privacy are part of every work day, privacy requirements and expectations will not be met and information security will be ineffective. A pervasive information security and privacy culture can be created and integrated into everyday job roles in three effective ways:

- Document information security and privacy responsibilities into job descriptions. This reinforces the reality that privacy and information safeguarding are not standalone operations that belong to someone else, but a responsibility that is expected of "me."
- Include information security and privacy within job appraisals. When it becomes personal—when everyone knows that their annual appraisals will include how well they protect PII—it's natural that diligence and compliance will increase. Confidential papers will be locked away. Computers will be locked when people are away from their desks. And it is likely they will think twice before sending PII in e-mail messages, or before loading PII onto laptops or flash drives.
- Include privacy and information security considerations into daily procedures. Incorporate privacy and information security checks into all procedures that involve handling or accessing PII.

Step 5: Implement cooperative awareness and training

Organizations will experience fewer incidents when the privacy and information security areas work together to implement cooperative awareness and training throughout the enterprise. Well-informed personnel not only have the knowledge to protect PII, but also training makes them more accountable for their actions.



A thoughtful, integrated education program should include:

1. Establishing benchmarks. Before launching training and awareness activities, measure information security and privacy awareness within your organization.
2. Developing targeted training applicable to job roles. Increase awareness across the organization to all staff and then provide customized, targeted training to those with significant responsibilities involving PII. These areas include, but are not limited to, call centers, marketing, IT, HR, and executive management.
3. Providing ongoing awareness communications and activities. Training must be complemented with ongoing awareness communications to reinforce information security and privacy requirements, and to keep these issues top-of-mind in day-to-day work.
4. Evaluating how well awareness has been raised. Training events and awareness activities must be evaluated to determine how knowledge has increased and identify where improvements and effort are needed.

Information security and privacy convergence improves business

It is critical for those responsible for information security, privacy, and the associated legal and compliance requirements to work closely together in partnership. Without this collaboration, organizations will operate inefficiently, with conflicting policies and directives. More importantly, there will be privacy and information security gaps ready for exploitation.

Successful programs require information security and privacy to have complementary strategies that are integrated enterprise-wide—within every business process and at every level within the organization. When information security and privacy work together and collaborate, there are fewer incidents, less negative business impact, and business is improved.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, has provided information security, privacy and compliance training, services, tools and products to organizations in a wide range of industries throughout the world for more than 17 years. Rebecca was named one of the "Best Privacy Advisers" in two of three categories by Computerworld magazine and one of the "Top 59 Influencers in IT Security" for 2007 by IT Security magazine. She is an author and adjunct professor for the Norwich University Master of Science in Information Assurance (MSIA) program. rebeccaherold@rebeccaherold.com; www.privacyguidance.com.



Share This

© 2017 International Association of Privacy Professionals.
All rights reserved.

Pease International Tradeport, 75 Rochester Ave, Suite 4
Portsmouth, NH 03801 USA • +1 603.427.9200

[Contact Us](#)

[Press](#)

[Advertise](#)

[Privacy statement](#)

[Refund policy](#)