# Are You Privacy Savvy?
# Determining Your Organization's Privacy Practices Grade

Rebecca Herold, CISM, CISSP, CISA, FLMI

(Note: Originally published in the November 2002 CSI Alert)

Most organizations, regardless of where they are located in the world, are increasingly subject to privacy laws and policies that regulate the collection, use and disclosure of personal information. Additionally a wide array of recent public opinion surveys consistently demonstrate that people are concerned about the privacy of their information in every aspect; related to being consumers as well as employees. So, are you on top of all the privacy issues that apply to your organization? It is vital today's society to know how to implement security appropriately and adequately to help reach compliance with the cornucopia of privacy legislation and regulations.

To help determine your privacy savvy as it applies to your organizational responsibilities as a security and/or privacy leader, here is a short self-evaluation. This is far from comprehensive and lacks the detail you will need to adequately address your privacy issues. However, it should help you see from a very high level where you need to start addressing privacy issues and concerns.

1. Is your industry governed by any existing U.S. or international privacy regulatory requirements?
   O Yes O No O Don't Know
2. Has a position within your organization been formally established to be responsible for staying up-to-date with and responsible for privacy issues and compliance?
   O Yes O No O Don't Know
3. In the past three months have you (or someone else) reviewed or updated the list of information security and privacy laws that apply to your organization?
   O Yes O No O Don't Know
4. Do you have a customer privacy policy that outlines how your organization will handle and protect customer information and confidentiality?
   O Yes O No O Don't Know
5. Do you prohibit the use of social security numbers (SSNs) or social insurance numbers (SINs) as your customer identifiers?
   O Yes O No O Don't Know
6. Do you allow customers to opt-out or opt-in for sharing personal information?
   O Yes O No O Don't Know
7. Do you allow customers to examine the personal information you have on file for them, and allow them to request corrections?
   O Yes O No O Don't Know
8. Have you classified the information processed within your organization to identify personal and confidential information?
   O Yes O No O Don't Know
9. Have you performed a data flow analysis for the personal and confidential information processed within your organization?
   O Yes O No O Don't Know
10. Do you know the security and privacy practices of the third parties who have access to your identified personal and confidential information?

 

O Yes O No O Don't Know

11. Are security and privacy requirements included at the beginning of each of your organization's systems development projects and incorporated into the solution?
O Yes O No O Don't Know
12. Do you have an employee privacy policy that communicates to your personnel what they can expect with regard to their personal privacy within the workplace?
O Yes O No O Don't Know

The impact for each of these questions varies; some of these issues are more substantial than others. However, for the purposes of this column, I am generalizing the results to fit the space allowed. So now, for the admittedly unscientific interpretation of the results of your self-assessment quiz…drum roll please…thrrddddddddd …

If you answered mostly "yes" to these questions, you are an awesome privacy-savvy guru; great job! Your grade in this situation is in the A/B range. Go back and look at the questions you answered with "no" or "don't know" and make it part of your to-do list to find the answers.

If you answered mostly "don't know" to these questions, you join the majority of people who are taking this quiz. Your grade in this situation is INCOMPLETE. You need to set aside some time and determine the answers to the corresponding questions.

If you answered mostly "no" to these questions, you need to seriously examine and address your organization's privacy policies and practices, and do so soon. Your grade in this situation is most likely in the D/F range. There is just too much at stake in today's business environment for any organization to dismiss privacy issues. With specific regard to question 1, you would be hard-pressed to find an organization for which no legislative or regulatory information security or privacy requirements apply. If you believe this is the case for your situation, please let me know! I'll be happy to eat crow and admit my error in an upcoming column.

You should give numbers 1, 5 and 10 in this self-assessment priority and address them soon. The others are also important, but will fall into line behind these issues.

Now that you've completed a very high-level assessment of your privacy activities and requirements, you should consider performing a privacy impact analysis (PIA) to get the details you need to create an effective privacy plan. A PIA is a structured, comprehensive project that determines if an organization's current or planned technologies, policies, procedures and systems meet the organization's established privacy policies as well as applicable legislative and regulatory compliance. The primary goal of a PIA is to effectively identify and communicate existing privacy risks that exist and those that are not being addressed. It will also help your organization to anticipate customer reaction or concern to privacy implications related to how their information is handled.

 

# Are You Privacy Savvy?
# Determining Your Organization's Privacy Practices Grade

Rebecca Herold, CISM, CISSP, CISA, FLMI

Remember, privacy impacts your organization in many more ways than just potential legal fines and penalties. As you create your organizational privacy plan, keep the following in mind:

- Personnel satisfaction – An employee who feels their privacy rights are being honored and that their employer is being forthright and honest about how their information is used is more likely to be productive, loyal and stay with your organization instead of looking for greener pastures elsewhere. Take care to ensure personnel information privacy.
- Customer satisfaction – A happy customer is more likely to stay a customer. An unhappy customer is more likely to pursue litigation. Take the necessary measures to ensure customer information privacy.
- Privacy policy wording - Consult with your organization's legal counsel to review privacy policies and procedures to make sure you are not promising something that cannot be feasibly fulfilled. Take care when wording privacy policies.
- PIA - Perform a privacy impact analysis. If you do not have the staff or expertise within your organization, hire a competent third party to perform the analysis. Take time to evaluate your privacy activities and requirements.
- Privacy non-compliance - Consult with your organization's legal counsel and auditors to review how customer and employee private information is being used, and if it is in conflict with your privacy policies. Take actions to ensure compliance.
- Privacy awareness - You cannot expect policies to be followed if they have not been communicated. Establish an ongoing privacy policies communication and awareness program. Take actions to increase and ensure privacy awareness.
- Practice what you preach - Incorporate privacy protection into your corporate values. Include information about privacy in your employee and management handbooks and other publications. Take time to walk the walk.
- Responsiveness - Respond to privacy (as well as security) breaches immediately. Ensure procedures exist to respond to privacy non-compliance incidents and media reports related to your organization's privacy practices and capabilities…or claims of the non-existence of such. Take necessary actions for privacy incidents.

 

# Are You Privacy Savvy?
# Determining Your Organization's Privacy Practices Grade

Rebecca Herold, CISM, CISSP, CISA, FLMI

Sidebar:

To help boost your privacy savvy, here is a partial list of privacy regulations with which you should become familiar. Some of these are very specific to industry, and others apply across a spectrum of industries. With which of the following regulations are you familiar?

- Children's On-line Privacy Protection Act of 1998
- Consumer Credit Reporting Act of 1996
- Driver's Privacy Protection Act of 1994
- Electronic Funds Transfer Act
- European Union Data Protection Directive of 1995
- Fair Credit Reporting Act of 1999
- Family Educational Rights and Privacy Act
- Federal Trade Commission Act
- Freedom of Information Act
- Gramm-Leach-Bliley Act of 1999
- Health Insurance Portability and Accountability Act of 1996
- Personal Information Protection and Electronic Documents Act (Canada)
- Privacy Act of 1974
- Telemarketing and Consumer Fraud Abuse Act
- Telephone Consumer Protection Act
- USA Patriot Act of 2001
- Video Privacy Protection Act

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant, author and instructor. She can be reached at rebeccaherold@rebeccaherold.com or 515-491-1564. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," and authored "Managing an Information Security and Privacy Awareness and Training Program" all published by Auerbach.

 