InformationShield

What Is The Difference Between Security and Privacy?

By Rebecca Herold, CISSP, CISA, FLMI

This article was previously published in the CSI July 2002 Alert newsletter.

Privacy versus Security

I've heard and overheard security professionals from many different organizations discuss security and privacy, and many of them are of the opinion that these two terms are one and the same. Then, on the opposite side of the spectrum, I've also heard many discuss how they believe security and privacy are diametrically opposed to each other. They are neither.

Many organizations have the people responsible for privacy completely separated from and in entirely different departments from the people responsible for security. Often these departments do not communicate, or even acknowledge or understand the compelling relationship that essentially exists between the two. Too often privacy is considered a purely legal issue, the responsibility for which is often handed to organizational legal counsel. Or, it is ignored altogether as a separate issue, and management assumes will be addressed by all the various business units during the course of doing business. Security is too often viewed as a purely technical issue, and the responsibility for security is more often than not placed within the information technology and/or networking support area…often buried beneath several layers of management. And, then the twain never meets. Security personnel must actively be involved in privacy issues and crafting privacy policies, and privacy personnel must be actively involved in security issues and crafting security policies.

The ideal situation is to have a Chief Privacy Officer (CPO) positioned at a high level within an organization, filled by a person is security savvy; and a Chief Information Security Officer (CISO) positioned at the same high level within the company who is privacy savvy, and the two communicate often and are in sync and active participation with each other's goals and activities. Yes, this would typically place the CISO at a level equal to the CIO, not

reporting to the CIO position. If your organization is large enough to support this structure, this is a very good thing! Placing the CISO high in the management structure clearly communicates to the organization, at all levels, that security is serious and a much broader concern than just technological, and it also helps to eliminate the conflict of interest that can so easily happen when security is placed within the CIO's domain.

So, to the crux of this article…how is security different than privacy? It's really pretty simple…you must implement security to ensure privacy. You must use security to obtain privacy. Security is a process…privacy is a consequence. Security is action…privacy is a result of successful action. Security is a condition…privacy is the prognosis. Security is the strategy…privacy is the outcome. Privacy is a state of existence…security is the constitution supporting the existence. Security is a tactical strategy…privacy is a contextual strategic objective. Security is the sealed envelope…privacy is the successful delivery of the message inside the envelope. Well, before I digress too far off the information path, I think I'll stop with the metaphors and assume you understand what
I'm trying to get across. Bottom line; enterprise privacy management strategies and security management architecture must be effectively and actively integrated.

What's a common mistake organizations make that can lead to potentially huge fines and lawsuits? Often, when the privacy responsibility lies in a different part of the organization from the security responsibility, or the two areas do not communicate, privacy policy notices are issued, then no security policies, procedures or mechanisms are implemented to ensure the now-published privacy policies are enforced. These published privacy policies are in effect a contract with your customers and consumers. The privacy policies are often the first and/or main point of contact between your customers and your organization. If you are telling your customers that your organization is performing certain activities to ensure their privacy, then you better well make sure your organizational personnel KNOW what they have committed to, whether or not they were involved with the privacy choices.

Privacy with respect to many of the current legislated regulations, such as HIPAA and GLB, means people are able to make informed choices when seeking care and reimbursement for healthcare based on how personal health information may be used, or are able to make choices about how their personally identifiable financial information is used and shared by the organizations with which they do business. Privacy enables patients to find out how their information may be used and what disclosures of their information have been made. Privacy enables consumers to find out how financial information is going to be protected and know that the people handling their information have been properly trained to protect their privacy. Privacy generally limits release of information to the minimum reasonably needed for the purpose of the disclosure. Privacy gives people the right to examine and obtain a copy of their own personal records and request

corrections. Privacy of personal information, contrary to common belief, is NOT a constitutional guarantee.

Security with respect to these same regulations constitutes those reasonable and prudent policies, processes, steps and tools that are used to maintain confidentiality and privacy. It involves all methods, processes, and technology used to ensure the confidentiality and safety of the once private information that has been entrusted to a third party by the customer or patient.

There are a slew of proposed privacy laws currently in effect and being considered by the U.S. Congress and multiple states; and internationally there are dozens of privacy laws that are in effect, or are on the verge of being implemented. Most, if not all, include security requirements to ensure privacy. Yes, security and privacy are not the same things, but they are inextricably related. They're kind of like a house…without a good foundation and footings (security), you will not have a stable dwelling (privacy). Your carpenter must be in constant and effective communication with your architect so you do not end up living in a house of cards.

About the Author

Rebecca Herold, CISSP, CISA, FLMI is an independent information privacy, security and compliance consultant, author and instructor. Rebecca has over 15 years of privacy and information security experience, and assists organizations of all sizes with their information privacy, security and regulatory compliance programs. She is the author of several books including *"Managing an Information Security and Privacy Awareness and Training Program"* and is currently authoring a privacy governance tool for Information Shield. For more information, Rebecca can be reached at rebeccaherold@rebeccaherold.com.