International Data Privacy Day is January 28 – Are You Leaving Yourself Open for a Breach?

The Privacy Professor Uncovers the Top Five Privacy Predictions for 2011

As electronic privacy becomes increasingly complex (Google, Facebook and countless large corporations have had substantial incidents and breaches), it's more crucial than ever that consumers and businesses understand their exposure and take steps to ensure their information is not compromised.

This Friday, January 28 is Data Privacy Day, as recognized by governments and technology leaders around the world. Based in Iowa, Rebecca Herold, The Privacy Professor, worked with the governor's office in an effective crusade to get the day declared again this year. Then, Herold then went one step further and launched a new educational website, www.secureyourwireless.org, a one-stop resource for understanding current wireless threats – and exposing infractions.

To honor Data Privacy Day, kick off the year and her new site, Herold reveals the top five privacy predictions for 2011:

1. All types of organizations must consider the risks involved with using cloud services.
More organizations will use outsourced cloud (remote computing and storage) services. Particularly small and medium-sized companies will move their information security and IT functions to outsourced cloud services because they simply do not have the expertise internally to effectively manage security and privacy, and cannot afford to hire traditional hourly consultants to help them. This will also be the case within education institutions currently struggling with budget cuts. Cloud services can be quite secure, but some simply aren't. Organizations must know the right questions to ask, and get satisfactory answers, prior to signing up for one.

2. Every organization is affected by social media sites.
Companies will use social media sites even more to communicate about their services and practices, and as a result of human error, malicious intent or even lack of knowledge, there will be significant privacy breaches (unauthorized use or release of personal information) through social media sites. Companies must ensure they have policies and supporting procedures in place for their personnel to follow with regard to posting (and actually not posting) information about the business, coworkers, customers and clients, even when employees are away from work and using their own computers. Policies and procedures will be most effective when communicated with ongoing awareness activities.

3. Healthcare privacy issues will become more problematic and come under heavier scrutiny.
Healthcare providers that qualify are all clamoring to get their $44,000 in "meaningful use" stimulus funds to convert to electronic health records. As part of the requirements for the funds, providers must perform an information security risk assessment and then fix any problems discovered. Plus, providers and their business associates (accounting firms, ad agencies, financial institutions, etc.) are going to be held to stricter compliance regulations due to changes in HIPAA and the HITECH Act. This will ultimately be good for consumers, but the transition to electronic records, even with these additional privacy

protections in place, will result in more patient information breaches if providers do not implement safeguards in a comprehensive manner, and ensure their business associates do the same.

4. All organizations that collect, store or handle personal information will increasingly perform privacy impact assessments to determine how to best address their individual circumstances.
These assessments will emerge as a corporate necessity, with utilities companies leading the way. For example, as utilities start converting their customers to smart meters and connecting to the Smart Grid, and as manufacturers create new types of smart appliances, they are going to find themselves faced with a large number of hurdles to prove their offerings are secure and protecting consumer privacy. Performing privacy impact assessment will help them to most effectively identify the risks and implement appropriate protections.

5. All organizations must address the risks inherent with mobile computing.
It would be hard to find a company today where personnel are not using mobile computers, smart phones or electronic storage devices. This use, and working away from the office, will continue to increase dramatically in 2011. Large amounts of sensitive and confidential information is often stored on such devices. Mobile computers and storage devices are very easy to misplace, to lose or forget, and are a favorite target of thieves. Appropriate security must be in place to protect them, and the information stored within them.

The weakest link in information security and privacy is people. Multiple studies show that most incidents and breaches occur because people simply didn't know what they were doing, they made a silly mistake, or they had ill intent because they knew that, with lack of privacy awareness, they would likely not get caught. Informed and aware personnel are countermeasures against security incidents and privacy breaches. Many laws and regulations explicitly require formal, ongoing training and awareness – not only HIPAA, HITECH, and GLBA, but also many other federal, state and local level laws, regulations and industry standards. Fines and penalties will become increasingly more significant for organizations that lack effective training and awareness activities.

To learn more about protecting your organization, please visit www.privacyguidance.com. There you'll find tips as well as educational vehicles and programs, such as Security Search, a fun, interactive and ongoing training activity based on one of CSI's Information Security Programs of the Year, which Herold designed for a Fortune 500 company.

Rebecca Herold, The Privacy Professor, is an information privacy, security and compliance consultant, instructor and author who has published 14 books and over 200 articles in her field. Rebecca is a world-renowned industry spokesperson whose accomplishments include:
• Leader of the federal government's NIST Smart Grid Cyber Security Privacy Subgroup
• Created the first cloud computing HIPAA/HITECH compliance platform for small businesses
• Named to "Best Privacy Advisers in the World" by Computerworld
• Recognized among "Top 59 Influencers in IT Security" by IT Security
• Acknowledged in "Eight Privacy Firms to Watch" by Computerworld

- Winner of The CSI Information Security Program of the Year
- Adjunct professor, NSA-certified Norwich University Master of Science in Information Assurance
- Certifications: CIPP, CISSP, CISA, CISM, FLMI

Contact:
Rebecca Herold
Rebecca Herold & Associates, LLC
Phone: 515-491-1564
rebeccaherold@rebeccaherold.com