

## **Handling Complex and Difficult Privacy and Information Security Issues**

**Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI**

**Christopher Grillo, CISM, CISA, CPA, ITIL**

### **Presentation Overview:**

Handling complex and difficult Privacy and Information Security issues has moved to the top of the list for companies maintaining customer and employee information. However, there are often gaps in communication and coordination between Privacy and Information Security activities. These gaps create more complexity and bigger challenges for companies to handle as well as putting the organization at greater risk for incidents, along with contractual and regulatory noncompliance. Successful programs require the two strategies to be complementary and integrated throughout all of the enterprise—within every business process stage and at every level within the organization. This workshop will provide practical knowledge and tools to address complex privacy and information security issues within your organization as well as learn how other organizations are handling these Privacy and Information Security challenges. Through discussing key trends, legal requirements and frameworks that are common to both areas, attendees will learn how privacy and security teams can effectively work together. Participants will take away several resources and tools they can start using right away to help successfully meet these complex and difficult challenges.

## Time-Based Objectives:

### Day One

**Privacy and Information Security Trends.** We will discuss the evolution of privacy and security activities within businesses, and highlight several important trends for which businesses must be aware. We will define and discuss the Privacy and Security roles, responsibilities, and organizational challenges, as well as business processes that are most impacted by Privacy and Security processes and initiatives.

**Privacy Laws and Strategy.** We will provide an overview of the many laws that organizations must be aware of and address. We will also discuss effective privacy strategies and the business impact of privacy, including common regulatory and compliance issues.

**Information Security Strategy.** We will discuss effective Security strategies and the business impact of security, such as those relating to risk management and regulatory compliance. We will provide a practical method of incorporating industry best practices into any organization, and provide a toolset for creating

**Security and Privacy Roadmaps.** We will discuss the need for planning, documenting, communicating, and executing your security and privacy strategy.

#### Key Objectives:

- Instill understanding of privacy and information security issues and governance methodologies for best business impact
- Instill understanding of how to use existing governance frameworks to successfully integrate privacy and information security throughout the entire organization
- Instill understanding of the major privacy and information security common challenges and how to establish partnerships to most successfully address all the accompanying issues
- Learn the legal ramifications and necessary key compliance activities necessary to demonstrate regulatory and legal due diligence and establish a standard of due care that supports business success
- Learn to create an actionable roadmap for coordinating privacy and information security activities within the organization
- Instill understanding of the importance of partnering information security and privacy in incident planning, implementation, and execution.

#### Attendees Will Leave With:

- A valuable set of course materials that you will be able to use as a reference on an ongoing basis immediately upon your return to the office
- A ready-to-use information security and privacy program planning toolkit and sample framework that participants can customize to fit their organizational needs
- Sample IT controls for privacy and information security for regulatory compliance
- A usable information security and privacy posture assessment tool and visual roadmap generator
- Sample website privacy policy
- Privacy impact assessment worksheet
- A ready-to-use business partner and vendor security and privacy program assessment and due diligence toolkit
- A security and privacy contract clause considerations checklist
- A comprehensive listing of useful security and privacy references and resources

### Day Two

We will discuss at length the five most common overlapping privacy and information security areas that have the most impact to businesses. For the first common area we will discuss how privacy and information security policies and procedures must be in sync, and the issues involved with making them effective. The second common area will demonstrate the needs and values for privacy impact assessments and

information security risk assessments, and how the two types of activities should be coordinated to realize greatest business value. The third common area will address the critical need for business partner and vendor privacy and security program reviews and what to include within the associated contracts. Common area four will provide details about the systems development life cycle (SDLC) and how to effectively address privacy and security issues within every phase of an SDLC. Common area five will provide important information all organizations must know about incident response for both privacy and information security, in addition to providing the key components of an effective response plan. We will provide case studies and exercises throughout the day to support and demonstrate how these common areas impact business, and the ways in which privacy and information security must partner.

## Rebecca Herold Bio

Rebecca Herold, CISSP, CISM, CISA, FLMI is currently an information privacy, security and regulatory compliance consultant, author and instructor with her own company, Rebecca Herold, LLC. Rebecca has over 16 years of information privacy, security and regulatory compliance security experience, has created and implemented corporate strategies and programs and provided numerous security and privacy services to organizations in a wide range of industries throughout the world. Rebecca was instrumental in building the information security and privacy program while at Principal Financial Group, which was awarded the 1998 CSI Information Security Program of the Year Award. Rebecca was named one of the "Top 57 IT Influencers in 2007" by Information Security magazine for her blog at <http://www.realtime-itcompliance.com>.

Rebecca authored "The Privacy Management Toolkit," "The Privacy Papers," "Managing an Information Security and Privacy Training and Awareness Program," "The Business Executive Practical Guides to Compliance and Security Risks," "The Definitive Guide to Security Inside the Perimeter," and co-authored "The Practical Guide to HIPAA Privacy and Security Compliance" and "Say What You Do" in addition to chapters in several books and over 100 published articles. Since the beginning of 2001, Rebecca has authored a monthly privacy and regulatory compliance column in the CSI Alert newsletter.

Rebecca has created several seminars; two recent ones include: "Handling Complex and Difficult Privacy and Information Security Issues" and "Managing a Privacy Governance Program." Rebecca is an adjunct professor for the Norwich University Master of Science in Information Assurance (MSIA) program, and has been a frequent and requested speaker at organizations, conferences and seminars for the past several years. Rebecca can be reached at [www.privacyguidance.com](http://www.privacyguidance.com) or [rebeccaherold@rebeccaherold.com](mailto:rebeccaherold@rebeccaherold.com)

## **Christopher Grillo Bio**

Christopher Grillo, CISM, CISA, ITIL, CPA (*inactive*) is the Director of Information Security for Medica. Chris is a business focused and technically adept leader with over 12 years of experience in information security, privacy, risk management, audit, and IT consulting in various industries. Chris has a proven track record of implementing and maintaining effective information security programs in various industries.

Prior to joining Medica, Chris was the Director of Information Security at Pearson Education where he led the global Information Security Program. Chris also held Information Security management positions at highly diverse and regulated companies with business operations in energy, auto, finance, software development, and government. In addition, Chris served as Sr. Principal Consultant at Guardent and Canaudit, where he led comprehensive information security and privacy engagements.

Chris is the author of several seminars such as: Handling Complex and Difficult Privacy and Information Security Issues, Enterprise Security Management, Security Awareness, Acquiring Information Security Tools, and Auditing System Development. He has published several articles and has been quoted in popular magazines such as InformationWeek, Computerworld and the CSI Alert.

Chris is an active member in various Information Security and Audit Associations, Privacy groups, and has served as chairperson of the Computer Security Institute (CSI) Advisory Council.