Changing the Mindset: Creating a Risk Conscious And Security Aware Culture

Overview

Creating a risk conscious and security aware culture within an organization can provide more protection to an organization's information infrastructure and associated data assets then any technology or information security related control that currently exists. A risk conscious and security aware culture is key to protecting an organization's information infrastructure and associated data assets. Information threats and adversaries are more advanced and daunting than ever and show no sign of becoming less concerning in the future. In order to effectively address this issue, organizations must create and cultivate a culture and environment that embraces information risk management and security as a business benefit rather than another hurdle on the path to success. This session will focus on the key concepts and capabilities that should be considered when creating a risk aware and security conscious culture. Approaches, considerations, techniques, and case studies of organizations that have are in process of or have successfully created this type of culture will be presented throughout the session as well as discussions of current industry leading concepts and practices.

Syllabus

- Using Risk Management to Remove the Fear of Security
- Risk Management and Security vs. Security and Risk Management
- Business and Information Risk Profiles
- Fighting the Hype Cycle
- Security by Compliance – Fear the Auditor more than the Attacker
- Polices and Standards First, Controls and Technology Second
- Focus on The Protection Data and Business Process Not Technology
- Data Classification
- Users – Your Greatest Asset and Most Challenging Adversary
- Trust by Verify
- Oversight Board – Removing the Perception of the Ivory Tower
- Winning the Hearts and Minds
- Embrace but Educate – Turning No into Yes
- Personal Benefits
- Effective Reinforcement Methods
- Focus on What Really Matters – Threat and Vulnerability Analysis
- Effectively Managing Risk – Control Objectives and Controls
- Final Thoughts

Who Should Attend

- Individuals who would like to understand how to effectively develop and implement Information Risk Management and Security strategy.
- Business leaders who are responsible for Information Risk Management and Security within their organizations.
- Information security auditors and professionals who are responsible for providing oversight to Information Risk Management and Security solutions within an organization.
- IT Governance professionals who are developing and maturing their organizations capabilities.

What Audience Will Learn

- Key considerations when creating a risk conscious and security aware culture
- How to use risk management as a concept and tool to remove the fear of security in organizations
- The value and benefits of developing an information risk profile
- Understanding of the current behaviors of organizations and whey they exist in regard to information security
- Effective approaches to change behaviors and culture within organizations
- How to leverage users effectively as an beneficial asset in supporting risk management and security activities
- How to use threat and vulnerability analysis to identify and educate organizations on the highly probable and business impacting threats can effect them
- Using control objectives as an approach to effectively manage information risk in a way that will be embraced by organizations.

Prerequisites

- Fundamental understanding of Information Risk Management and Security
- Basic understanding of organizational behavior and reasons for their resistance in implementing and embracing information risk management and security concepts and capabilities.
- Knowledge of business, compliance, and regulatory requirements associated with Information Risk Management and Security

Presentation Time

- This presentation can be conducted in a 60, 75, or 90 minute period.

Instructor

John P. Pironti is the President of IP Architects, LLC. He has designed and implemented enterprise wide electronic business solutions, Information Risk Management and Security

strategy and programs, enterprise resiliency capabilities, and threat and vulnerability management solutions for key customers in a range of industries, including financial services, energy, government, hospitality, aerospace, healthcare, pharmaceuticals, media and entertainment, and information technology on a global scale. Mr. Pironti has a number of industry certifications including Certified in the Governance of Enterprise IT (CGEIT), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified in Risk and Information System Control (CRISC), Information Systems Security Architecture Professional and (ISSAP) and Information Systems Security Management Professional (ISSMP). He is also a published author and writer, highly quoted and often interviewed by global media, and an award winning frequent speaker on electronic business and information risk management and security topics at domestic and international industry conferences.