Top Five Things You Should Do Before You Buy Another Piece of Information Security Technology

Overview

Somewhere along the way information security become about buying the next great piece of technology to solve the problem or fill the box in the auditor's checklist. Unfortunately, this approach has yielded only nominal results to date and the challenges of information security and risk management are far surpassing any of the technology or compliance requirements we have today to solve them. Instead of moving the pieces of the puzzle around the board in a desperate effort to combat the technical and regulatory threats of today we should instead be trying to solve the puzzle to effectively and adequately address the information risks of both today and tomorrow. This session will discuss five key activities an organization can perform to truly enhance their information security and risk management capabilities prior to making the next purchase of the technology that they think will solve the problem by may ultimately become the problem.

Syllabus

- Why technology alone will never be able to conquer the challenge of information security and risk management
- Current State: Technology Focused and Compliance bound information security
- Desired State: Information Risk Management and Security
- Activity 1: Developing a risk profile for your organization
- Activity 2: Understanding your business by performing and maintaining business processing mapping
- Activity 3: Building and maintaining an accurate logical and physical asset inventory
- Activity 4: Performing and maintaining Threat and Vulnerability Analysis
- Activity 5: Identifying controls and capabilities which will help you align with your risk profile
- Final Thoughts

Who Should Attend

- Individuals who would like to understand how to effectively develop and implement information security and risk management capabilities
- Individuals who are seeking new approaches to information security and risk management

- Business leaders who are responsible for information Security and Risk Management within their organizations.
- Information security auditors and professionals who are responsible for providing oversight to Information Security and Risk Management solutions within an organization.
- IT Governance professionals who are developing and maturing their organizations capabilities.

What Audience Will Learn

- The reasons why information security technology alone cannot solve the information security problems that exist today.
- Current and desired states of information security and risk management
- Five Activities which they can perform to greatly enhance their information security and risk management capabilities before they purchase any new technology.
- Insights from case studies and operational experiences on how these capabilities greatly enhance the capabilities of organizations without enhancing their budget requirements or technology spend.

Prerequisites

- o Fundamental understanding of Information Risk Management and Security
- o Knowledge of business, compliance, and regulatory requirements associated with Information Risk Management and Security.

Presentation Time

- o This presentation can be conducted in a 45, 60, 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 security and risk management 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 a award winning frequent speaker on electronic

business and information security and risk management topics at domestic and international industry conferences.