Information Security Policies and Standards

June 7, 2018

This SecureTheVillage Webinar brought to you by …

Information Security Policies and Standards

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guest
  - John Stambelos, Principal, Stambelos Consulting, LLC

Today's Objectives

- The Vital Role Played by Information Security Management Policies and Standards

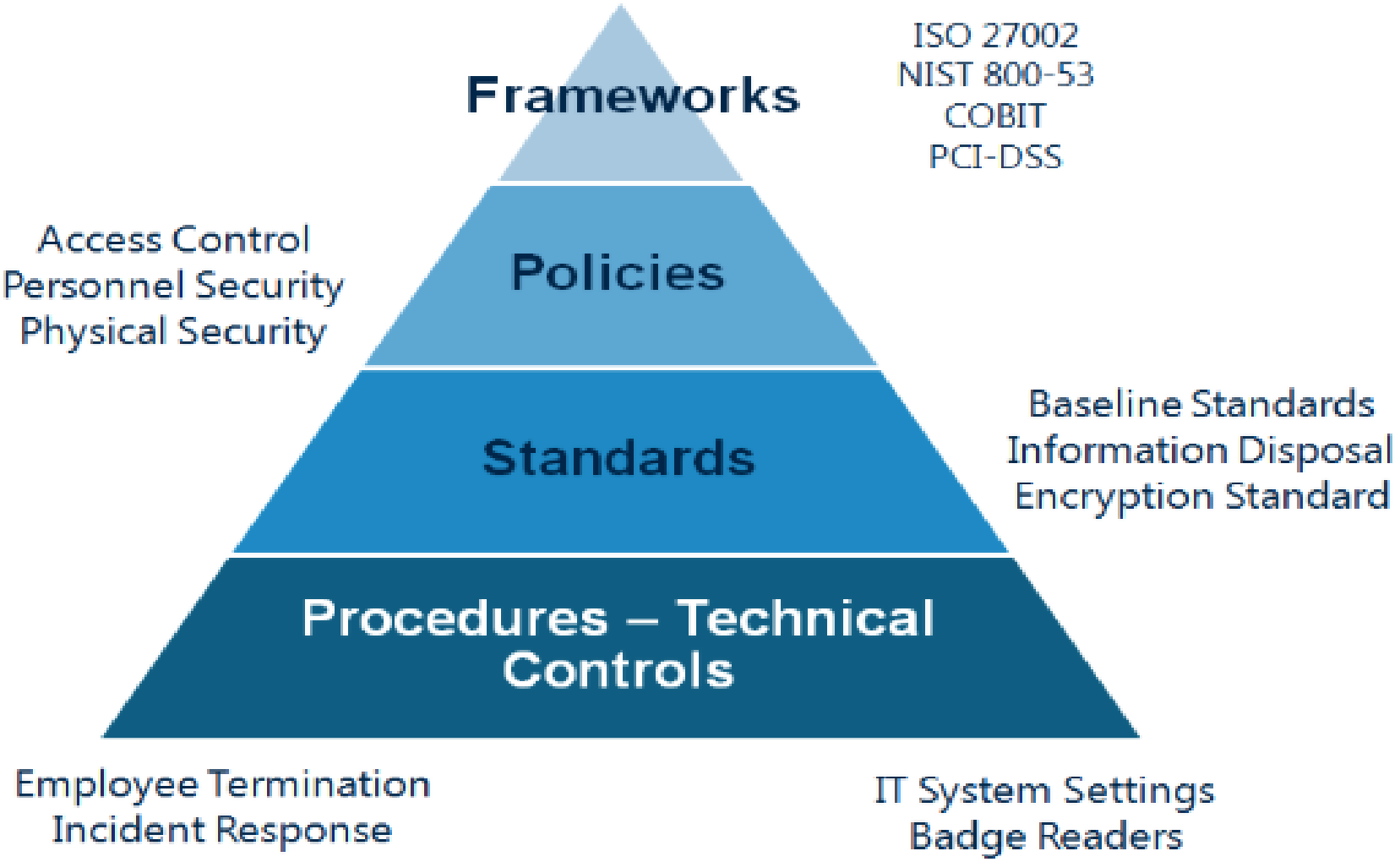
Things We'll Talk About

- Why information security policies are mandatory
- What your information security policies need to include
- How to develop, implement, and maintain information security policies
- Short. Sweet. And to the Point …. or … Everything but the Kitchen Sink.
- Policies and Standards. What's the difference. And why it matters.

Getting Started

Information Security Management Policies and Standards are the key strategic management framework supporting commercially-reasonable information security management practices for organizations of all kinds.

The Politics of Standards …
The Hierarchy of Nomenclature



Source: Information Shield (The Hierarchy of Security Policies, Standards and Procedures)

Policies, Standards and Procedures (oh my!)

High Level Governance

Practical Details

Step-by-Step Instructions

- Characteristics of Policies:
  - High-level governance statement
    - Ex: Accounts must have strong passwords
- Characteristics of Standards:
  - Necessary level of detail to be practical
    - Ex: 12-character passwords with complexity
- Characteristics of Procedures:
  - Step-by-step instructions to follow
    - Ex: Select Ctrl-Alt-Del and choose “change”

Why Information Security Policies are Mandatory

- Required to meet compliance obligations
- Defines your organization's approach to managing information assets
- Describes how you manage information security
- Documents management responsibility, accountability, and authority
- Lays out clear rules for workforce behavior
- Describes consequences for noncompliance
- Provides basis for evolving cyber-aware culture

Things Your Information Security Policies and Standards Need to Include

- Security Management & Governance
  - How you manage / govern
  - Annual risk assessment
  - 3rd-party security management
- Information Classification and Control
- User Security
  - Acceptable Use
  - Security awareness and training
  - Consequences of failure
- Human Resources
- Physical and Environmental Security
- IT Infrastructure Security
  - Vendor security management
  - Network architecture
  - Device protection
  - Vulnerability and patch management
  - Asset management
  - Identity and access Management
  - Logs and Log management
  - Incident event management
  - Business continuity and disaster recovery
  - Change and configuration management

How to Develop, Implement, and Maintain Information Security Policies

- Obtain top-level executive support and authority
- Focus on protecting information
  - Information categories
  - Legal, financial, and other requirements for different information categories
  - Confidentiality, Availability, Integrity
- Make policies practical
- Develop in coordination with key stakeholders
  - Security is a team effort; *It Takes the Village*
- Minimize details – policies should not change often
- Include Mechanisms for Decision Making & Change
  - Accept, transfer or reject risk
  - Waive or add a new policy or standard
  - Require annual review
- Don’t hand them out if you can

Short. Sweet. And to the Point…or… Everything but the Kitchen Sink?

- Minimize details (those belong in procedures)
- Minimize jargon and use straightforward language
- Don’t include it if you can’t do it
- Include only enough to accomplish your objectives
- Imagine if your policies were subpoenaed
- Match your corporate culture (or change it)
- Remember what new employees will need to read
- Remember they will be circulated annually

Next Webinar: Conducting an Information Security Risk Assessment

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- June 29, 10AM Pacific
- Registration: SecureTheVillage.org

SecureTheVillage Webinar Series

- Information Security Management Guidance
  - Practical
  - Real-World
  - How-To
  - Actionable
- SecureTheVillage ResourceKit
- First Thursday of month, 10AM Pacific

Information Security Management Webinar Schedule — 2018

February 1	Information Security Management Overview; The Role of Leadership
March 1	The Information Security Management & Leadership Team
April 5	*Online Bank Fraud — How To Avoid Being a Victim*
May 3	*Basics of Cyber-Law*
June 7	*Information Security Policies and Standards*
June 29	**Conducting an Information Security Risk Assessment** [Date Change due to July 4th]
August 2	Information Classification and Control
September 6	Securing the Human
October 4	Managing Security of the IT Infrastructure
November 1	Getting Cyber-Prepared : Incident Response & Business Continuity
December 6	Third-Party Security Management
January 2019	Managing Cyber-Risk and Insurance

SecureTheVillage: Turning People and Organizations into Cyber Guardians

Monthly Webinar Series: Provides Practical Real-World Actionable How-To Information Security Management Guidance.

Executive Focus Groups: Designed to assist Chief Executives meet their responsibility for creating a cyber resilient culture.

Information Security Management and Leadership ResourceKit: A practical guide for implementing an information security management and leadership program in your organization.

Code of Basic IT Security Management Practices: A set of basic IT security management practices that are so basic that a failure to implement them puts the organization at a dangerous and unnecessary risk of a costly information incident.

Community-Based Programs to train the broader community in basic cybersecurity defense practices for themselves and their families, helping them become cyber-aware citizens.

Visit us at: *SecureTheVillage.org*

For More Information …

Stan Stahl, SecureTheVillage & Citadel Information Group
Stan@SecureTheVillage.org
323-428-0441

John Stambelos, Stambelos Consulting LLC
john@stambelos.com
(213) 725-3493