The Information Security Management & Leadership Team

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group

- Guest: Dennis Duitch
  - Duitch Consulting Group
  - SecureTheVillage Leadership Council

- Webinar Topics:
  - Team Mission, Goals, and Objectives
  - Team Membership, Chair, and Meetings
  - Team Operations
  - Team Authority, Accountability, and Governance
Webinar 1 Summary

- **Objective:** Manage Information Risk
- **Why:** Information Risk Leads to Business Risk
- **Protect:** Confidentiality, Integrity, Availability
- **The Need:** Secure The Human
- **The Need:** Secure the Technology
- **To Do:** Create a Cybersecurity Culture
- **How:** The NIST Framework
- **How:** The Seven Critical Management Strategies
- **How:** The Information Security Manager
- **How:** Cross-Organizational Information Security Management & Leadership Team
- **Key to Success:** CEO Leadership
The number one thing at the Board level and CEO level is to take cybersecurity as seriously as you take business operations and financial operations. It’s not good enough to go to your CIO and say “are we good to go.” You’ve got to be able to ask questions and understand the answers.

Major Gen Brett Williams, U.S. Air Force (Ret)
This Week with George Stephanopoulos, December 2014
“Finding good players is easy. Getting them to play as a team is another story.”

~Casey Stengel
1890-1975
American Major League Baseball outfielder & manager
A Few Things That Get in the Way

- Must Overcome Myth That Information Security is Something IT Takes Care of
- Information Security Management is a Part-Time Job
- Team Members’ May Have Different Organizational Priorities
- Team Members Already Have Primary Responsibilities: These May Need to Be Aligned With Information Security
- Security Manager Must Keep Team Members Involved, Engaged, and Enthused
Only three things happen naturally in organizations: friction, confusion, and underperformance. Everything else requires leadership.

— Peter Drucker —
The Information Security Management & Leadership Team: The Framework

What ... Who ... When ... Ops ... Governance
Team Mission

- Responsible for managing the organization’s risk-based Information Security Management Program.
- Responsible for organizational leadership in creating a cybersecurity culture.

Good business leaders create a vision, articulate the vision, passionately own the vision, and relentlessly drive it to completion.

Jack Welch
Team Goals

- Ethical Responsibility
- Proportionate Risk
- Commercial Reasonableness
- Organizational Completeness
- Minimize Operational Impact
- Cost-Effectiveness
- Continuous Improvement
Team Objectives

- Information Security Policies and Standards
- Staff awareness, cybersecurity culture
- Manage IT security management
- Vendor and 3rd-party security management
- Information resilience
- Support staff with information security tools (e.g., password management tools)
- With Finance Department, manage risk of online bank fraud.
- Compliance
- Cyber-insurance
- Support business development
Chase Perfection

Perfection is not attainable, but if we chase perfection we can catch excellence.

Vince Lombardi
Team Membership: Cross-Functional to Cover Entire Organization

- **Team Members**
  - Information Security Manager (ISM) (Chair)
  - Chief Operating Officer
  - Chief Financial Officer
  - IT Director
  - Director of Human Resources
  - Director of Development (nonprofit)
  - Chief Risk Officer (if present)
  - Chief Legal Officer (if present)

- **Subject Matter Expertise**
  - Information security management
    - Different from IT
  - Cyber law
  - Cyber insurance
Structure Reflects Management / Leadership Challenges & Responsibilities

1. Leadership / Governance
   - CEO

2. Management
   - Information Security Manager
   - Operations
   - Finance
   - IT

3. Steering Committee
   - Install Management
   - Cultural Adaptation
   - Augment w Security
   - Cultural Adaptation

Subject Matter Expertise
The Three Phases of Information Security Implementation

- **Phase 1: Get Started**
  - Duration: 2 - 3 Months
  - Build Security Management Foundation

- **Phase 2: Grow Discipline**
  - Duration: 3 - 4 Months
  - Implement Security Management Practices

- **Phase 3: Steady-State**
  - Continuous Improvement
Basic Operations: Getting Started

- Initial Team Training
- Implement information security management policies and standards
- Provide basic awareness training to staff
- Conduct an Information Security Risk Assessment
- Develop Findings and Recommendations

- 1 – 3 months
“The most common source of mistakes in management decisions is the emphasis on finding the right answer rather than the right question.”

Peter Drucker
Basic Operations: Develop the Initial Action Plan

- Develop an *Initial Action Plan* based on *Findings and Recommendations of Information Security Risk Assessment*
  - Much of it will likely focus on IT
    - IT Security Management Subcommittee
      - ISM
      - Head of IT
      - Person to whom Head of IT report?
- What’s to be done in the next 3 months?
- What’s to be done in the next 6 months?
- What’s to be done in the next 12 months?
Basic Operations: Monthly Meetings to Plan the Work & Work the Plan

- The Team, including its Subject Matter Experts, meets monthly
  - What was planned for the month?
  - What was accomplished?
  - What was the basis for being under/over?
  - What are the plans for next month?
  - What are the rolling plans for the next 3 months, 6 months and year?
Continuous Performance Improvement

The *Spiral Model*℠ of Continuous Performance Improvement

*Spiral Model* is a Service Mark of Citadel Information Group.
Team Authority, Accountability, and Governance

- **Authority**
  - In coordination with Chief Executive, authority to establish and enforce binding policies and standards
  - In coordination with CFO, authority to establish budgets, commit resources and direct expenditure of organizational resources

- **Accountability**
  - The Chief Executive (and Board) holds Team accountable

- **Governance**
  - Quarterly review meeting with Chief Executive
High Performance Teams
Coming together is a beginning; keeping together is progress; working together is success.

— Henry Ford —
“Talent wins games, but teamwork and intelligence win championships.”

- Michael Jordan
Blind men and elephant
Patrick Lencioni’s Five Team Dysfunctions

**Dysfunction of the Team**

- **Go First**
  - Absence of Trust
- **Mine for Conflict**
  - Fear of Conflict
- **Force Clarity and Closure**
  - Lack of Commitment
- **Confront Difficult Issues**
  - Avoidance of Accountability
- **Force on Collective Outcomes**
  - Inattention to Results

**Role of the Leader**

“Trust is knowing that when a team member does push you, they are doing it because they care about the team.”

- Patrick Lencioni

“Remember teamwork begins by building trust. And the only way to do that is to overcome our need for invulnerability.”

- Patrick Lencioni
“If everyone is moving forward together, then success takes care of itself.”

-Henry Ford
"You have to start by teaching the fundamentals," Lombardi said. "A player's got to know the basics of the game and how to play his position. Next, you've got to keep him in line. That's discipline. The men have to play as a team, not as a bunch of individuals. There's no room for prima donnas."

He continued: "But there have been a lot of coaches with good ball clubs who know the fundamentals and have plenty of discipline but still don't win the game. Then you come to the third ingredient: if you're going to play together as a team, you've got to care for one another. You've got to love each other. Each player has to be thinking of the next guy and saying to himself: 'If I don't block that man, Paul is going to get his legs broken. I have to do my job well in order that he can do his.'"

"The difference between mediocrity and greatness is the feeling these guys have for each other. Most people call it team spirit. When the players are imbued with that special feeling, you know you've got yourself a winning team."

Then he blurted out almost self-consciously: "But Lee, what am I telling you for? You run a company. It's the same thing, whether you're running a ball club or a corporation. After all, does one man build a car all by himself?"

*Vince Lombardi, Recounted by Lee Iacocca in his autobiography*
Assignment: Action Steps Prior to Next Webinar

- Identify the Information Security Management & Leadership Team
- Have all Team members watch this webinar
Next Webinar: Online Bank Fraud — How To Avoid Being a Victim

- **Guide:** Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group

- **Guest:** Barbara Allen-Watkins
  - Senior Vice President Treasury Management
  - City National Bank

- **April 5, 10AM Pacific**

- **Registration:** SecureTheVillage.org
SecureTheVillage Webinar Series

- Information Security Management Guidance
  - Practical
  - Real-World
  - How-To
  - Actionable

- SecureTheVillage Resource Kit
- First Thursday of month, 10AM Pacific
Webinar Schedule — 2018

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 Resource Kit:** 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  
Stan@SecureTheVillage.org  
LinkedIn: Stan Stahl  
323-428-0441  
Twitter: @StanStahl

Dennis Duitch  
dennis@DuitchConsulting.com  
LinkedIn: Dennis Duitch  
(818) 905-0275

Duitch Consulting Group  
duitchconsulting.com

Citadel Information Group  
citadel-information.com  
Free: Cyber Security News of the Week  
Free: Weekend Vulnerability and Patch Report

SecureTheVillage  
SecureTheVillage.org  
Executive Focus Groups  
Code of Basic IT Security Management Practices  
Information Security ResourceKit  
Webinar Series: 1st Thursday of Month
SecureTheVillage: Turning People and Organizations into Cyber Guardians