Out Thinking The Barbarians:

The Agile Cybersecurity Action Plan (ACAP)

PRESENTATION TO THE ICF INTERNATIONAL CYBERSCI SUMMIT

OCT. 14, 2015

JOHN W. LINK & JO LEE LOVELAND LINK

John W. Link & **Jo Lee Loveland Link** of **VOLVOX Inc.**

WE DO THE "HUMAN STUFF" OF IT :

ORGANIZATION DYNAMICS, STRATEGY AND STRATEGIC COMMUNICATIONS

FOR GOVERNMENT, CORPORATIONS AND NON-PROFITS

- *Jo Lee - Visiting Scientist CMU/SEI - CMMI, Risk Management, Managing Technology Change at NRO, Warner-Robins AFB, other agencies.*
- *Master of Applied Behavior Science, Organizational Systems Dynamics*

- *John - Army Chief of Staff for Installation Management (OACSIM) CIO - FEMA/CSEPP, DOJ, others.*
- *Master Conflict Analysis and Resolution, Organization Change Management, Enterprise Integration*

- *Both – Members, Senior Governance Team, DOD OSD CIO/NII Horizontal Fusion Portfolio Initiative, Johnson & Johnson Information Management Global Strategic Communications , others*

- *Co-designers - CHAOS, Inc. ™, original experiential learning laboratory*

Agenda

- Introduction
- Problem Definition: The Clash of Cultures
- What the Hell is an ACAP?
- The ACAP Process: Fresh Thinking
- ACAP: Success Factors
- How ACAP Transforms Cybersecurity Culture
- Advantages of the ACAP Approach
- Next Steps for ACAP

How Cybersecurity Sees Itself

How Cybersecurity Actually Is – Cyber-barbarians inside the Gates

The Cybersecurity Problem: Clash of Cultures

Cyber Adversaries: Inherent Advantages:

- Cyber Offense can bat .001 /Cyber Defense must bat 1.000
- Cheaper with Great ROI
- All against One: Multiple cultures and approaches
- Creative and Adaptive
- Share Information
- Criminal, Ideological and often Immoral

Our Cyber Defense: Inherent Disadvantages:

- "Compliance Culture" and Structural Factors
- Rigid hierarchies of decision making
- Compliance to National Standards known to our enemies
- Requires more rigid, button up folks to be clearable
- Users are people, people are idiots -fishing works
- Agile Methods still novel in conventional It

Inherent Tensions in Cybersecurity Culture

- Technical vs. human priority struggles
- Information secrecy vs. information sharing
- Adaptive vs. compliance
- Detail vs. speed
- Big picture vs. technical details
- The uncomfortable secret: Cybersecurity safeguards will likely not be 100% -- how to decide the core essentials to protect?

What the Hell is an ACAP?

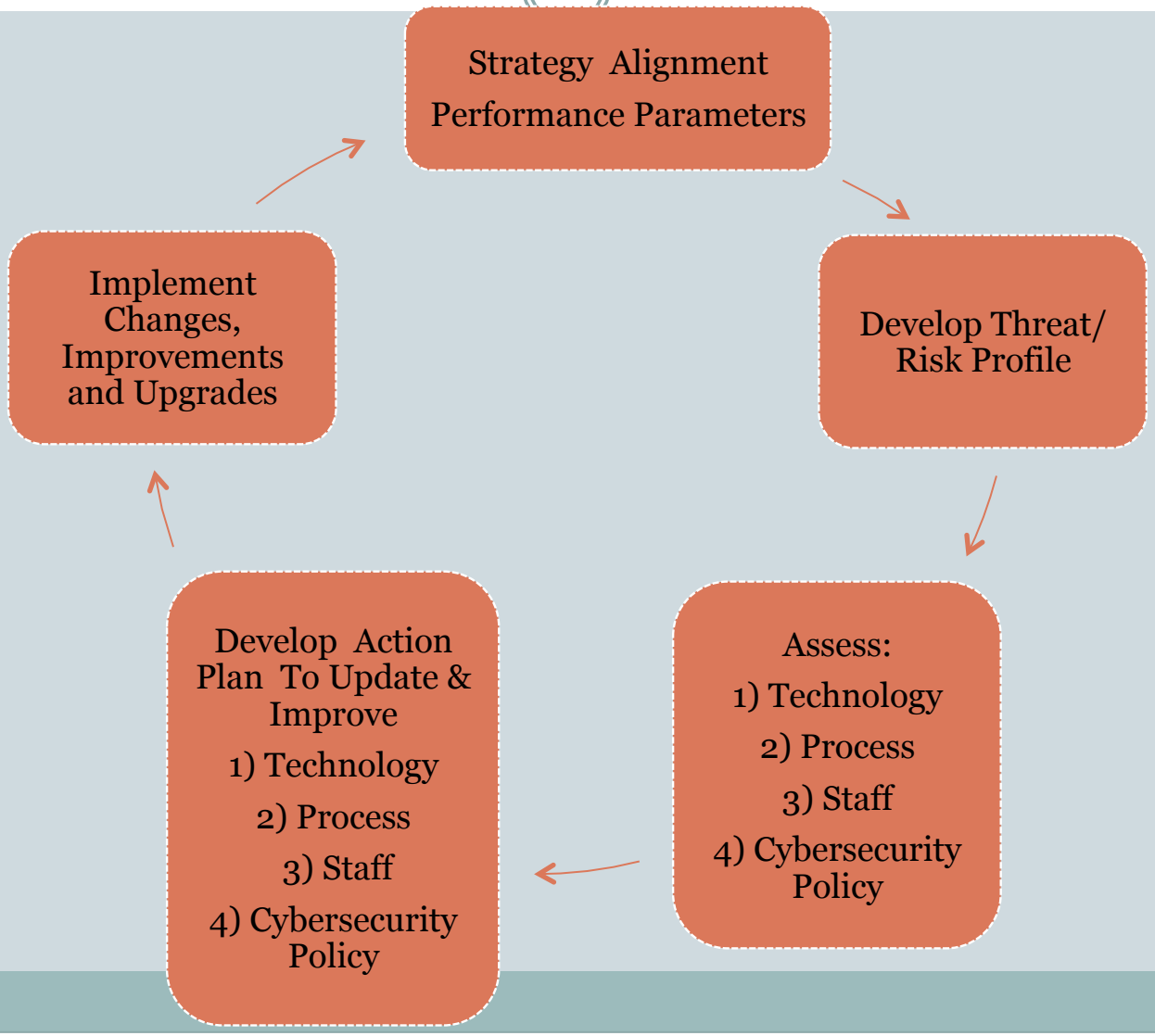
- Stands for **Agile Cybersecurity Action Plan**
- Facilitated multi-step process of an **ACAP Strategy Team**
- Iterated in 1-6 month cycles
- Critical Activity: Threat and Risk Matrix
- Assess/ revise iteratively Cybersecurity infrastructure:

  Technology, Processes, Staffing and Policy
- Active outreach: Users/ stakeholders/ community
- Primary ACAP Goal: Create Adaptive Cybersecurity Strategy
- Collateral ACAP Goal: Create more Adaptive Cybersecurity Culture

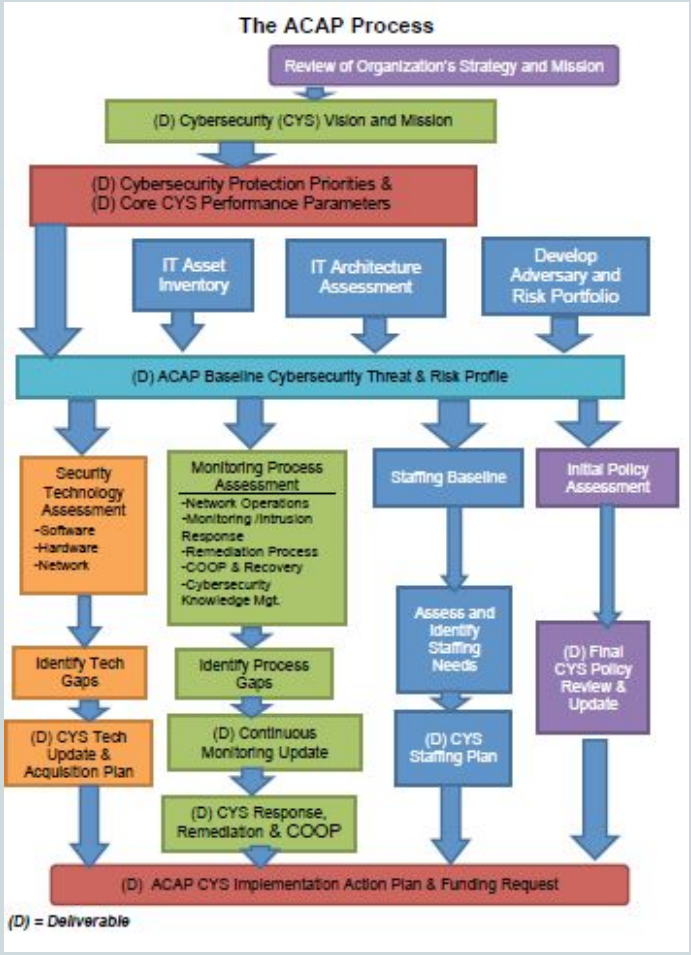
ACAP Process: Fresh Thinking

1. Create (and continuously update) **Threat/Risk Profile**
2. Assessment #1: Current Cybersecurity Architecture and Enterprise Architecture
3. Assessment #2: Cybersecurity Infrastructure (based on Threat/Risk Profile): **Technology**, **Monitoring Processes, Response Plans**, **Staff Capacity** and **Cybersecurity Policies**
4. Anticipate what could go wrong, and fix it before it does
5. Launch integrated **ACAP Action Plan**

Simplified ACAP Cycle



ACAP Process Chart



ACAP Success Factors

1. Rapid Execution and Agile Process
2. Senior Leaders Sponsorship and Active Participation
3. Multi-level Participation on ACAP Strategy Team
4. Professionally Facilitated Process
5. Use of Subgroups
6. Culture Transformation
7. Action Planning and Implementations
8. Use of Subject Matter Experts (SMEs) with ACAP Strategy Team:

- **Master Strategy Team Facilitator**
- **Organizational Change Management Expert**
- **Threat/Risk Management Planning Specialist**
- **Penetration Testers/ External White Hat Hackers**
- **Attorney-Advisors**

How ACAP Transforms Cybersecurity Culture

Organizational Culture = People's default beliefs about their organization (usually unexpressed) and behaviors

- Beliefs drive assumptions
- Assumptions drive decisions
- Decisions drive direction
- Direction drives behaviors
- Behaviors drive actions (planning, processes, rewards, etc.)

Changing Cybersecurity Culture

Compliance Culture

-Reports/shelfware
-Annual
-Adheres to Hierarchy
-Requirements Driven
-Budget Cycle
-Framework Driven
-SOP
-Reacts

Adaptive Culture

-Action
-Iterative quick cycles
-Collaborative Team
-Agile
-Need Driven
-Threat /Risk Driven
-Creative
-Anticipates

Advantages of the ACAP Approach

1. Enhanced Rapid Decision Making: ***Both Speed and Quality***
2. Focus on getting it done – quickness
3. Supports smart Cyber Technology Portfolio Management
4. Greater Coordination between Technology, Policy, and Budget
5. Agile Speed and Iteration: ***Try, Test, and Revise***
6. Levels the Playing Field of Ideas through Facilitated Dialogue
7. Increases the Likelihood That Undiscovered Breaches will be Discovered and Remediated
8. Creates ongoing System and Organizational Learning
9. Builds Organizational Resilience

Next Steps for ACAP

AS YOU SUSPECTED ….ACAP IS CONCEPT SPACE

We are looking for:

- Agencies, Non-Profits, or Corporations to pilot ACAP
- Academic partners to collaborate in building pilots and researching outcomes
- Together we create foundation for ACAP capacity-building
- The community continues further improvements to the ACAP process

Looking ahead:

- Congress should consider an ACAP as a due diligence for acquisition purposes to expedite Cybersecurity resource pipeline

Thank you!
Questions?

JOHN W. LINK AND JO LEE LOVELAND LINK
WWW. VOLVOXINC.COM
540-465-1491