Creating an Adaptive Cybersecurity Culture Through the Agile Cybersecurity Action Plan (ACAP)

John W. Link & Jo Lee Loveland Link

October 2015

ABSTRACT: Cybersecurity is operating in an environment of unpredictable accelerated technology change and growing threats. Often Cybersecurity planning and operations are based on out-of-date threat frames, approaches, and Strategies. Staid, traditional, narrowly-focused technical methods are promoted as protections against what are new, innovative, and ever-changing adversaries and approaches. To meet emergent Cyber threats, Cybersecurity protection Strategies must be holistic, agile, adaptive, and updated. To be successful, Cybersecurity must address the Cybersecurity Organizational Culture. Cultural and social dynamics inform Cybersecurity Strategy and Action. The dream of technical-only solutions must now be outgrown. Human intelligence and human problem-solving, information sharing, and collaboration must undergird the strategies for this increasingly turbulent environment. Federal Cybersecurity has relied on FISMA to drive Federal Cyberstrategy and have created a "Compliance Culture" across the Federal Cybersecurity community. Despite its improvements, the new Federal Cyber Framework tends to unintentionally reinforce the already rigid compliance culture that has characterized FISMA's history, in both government and now the private sector. Organizations with rigid compliance cultures are at risk of reduced creativity or ability to adapt to emergent conditions. The solution: The Agile Cybersecurity Action Plan (ACAP), which integrates a fusion of ideas from Agile Methodologies, Strategic Planning, Creative Thinking, Collaboration, Process Improvement, Threat/Risk Management, Portfolio Management, and Cybersecurity Best Practices. This holistic amalgam is necessary to create the alert, adaptive, and continuous cycle of iterative Cyberstrategies and resilient action planning needed to counter the new Cyber threat environment. ACAP Starts by identifying current and emerging Threats/Risks and creating counter-Strategies based on an analysis of the organization's technology, processes, policies and Staffing. ACAP brings together senior leaders, techies, specialists, and hopefully (in the spirit of true Agility) users, to pool knowledge, generate novel ideas, and make Strategic decisions collaboratively. Together, these sometimes conflicting, but ultimately mutually enriching, contributors can generate more adaptive and successful approaches to Cybersecurity management. ACAP lays the foundation for evolving the adaptive Cybersecurity organizational culture needed to successfully meet emerging Cyber threats.

Unclassified

The Agile Cybersecurity Action Plan (ACAP)

John W. Link and Jo Lee Loveland Link

Table of Contents

"We cannot solve our problems with the same thinking we used when we created them." Albert Einstein

The Agile Cybersecurity Action Plan (ACAP)

1.0 Introduction

Today's news headlines are full of Stories about cyber-attacks on DOD, the U.S. Energy Infrastructure, and American business. OPM, E-Bay and PayPal have been massively hacked in recent months. Over the 2013 winter holidays, card numbers and personal information of an estimated 70 million Target customers were stolen. Neiman-Marcus reported their networks were also breached and at least three other major retailers (yet to be publicly declared) were also attacked. Authorities believe this series of retail attacks originated in Eastern Europe. But attacks can come from anywhere – domestic as well as international. A recent survey by the Duke University School of Business/CFO revealed that 80% of all American corporations might have already been penetrated.

Cybersecurity today is driven primarily by a "Castle Model" of defense, focusing on building relatively static Cyber defenses of firewalls, applications, monitoring software, and rigid processes in hopes that, with some occasional tweaking, updating and remediation, these protections will hold. The somewhat misguided belief is that these are sturdy battlements and they just need some occasional maintenance.

However, we face two enemies: The multi-tribe, multi-variant armies of Cyber Barbarians outside the battlements, AND the bureaucratic lethargy and all-too-common paralysis within.

There is a gaping and urgent need for a new kind of adaptive organization that injects critical analyses, artful technology, policy, and process changes, creative thinking by actual people, and rapid implementation for success in the emerging Cybersecurity environment. This is where the **Agile Cybersecurity Action Plan (ACAP)** comes in.

ACAP begins with a Master-level professionally-facilitated 1-3 day process, where a cross-functional Leadership and Technical Team called the **ACAP Strategy Team** charged to develop a holistic Cyber Strategy based on a current Threat/Risk Model. The ACAP Strategy Team brings together **C-level participants** (CIO, CTO, and CISO), technologists, SME's or specialists from unorthodox and previously unanticipated fields, and thoughtful users to pool knowledge and novel ideas and make strategic decisions collaboratively. Together, these sometimes conflicting but ultimately mutually enriching contributors can create more adaptive and more successful approaches to Cybersecurity management. Applying elements of penetrating strategic insights – as well as "Think Tank" investigations, the ACAP Strategy Team provides high levels of knowledge sharing and creative thinking. Key tasks of the ACAP Strategy Team include:

1) Create and continuously update an organizationally unique, strategic, and continuously evolving **Threat/Risk Profile**.
2) Rapidly assess the organization's current Cybersecurity Architecture and Baseline Architecture for Cybersecurity flaws.

3) Assess at a deeper level the Threat/Risk Profile against the elements of the organization's Cybersecurity Infrastructure: **Technology**, **Monitoring Processes, Response Plans**, **Staff Capacity** and **Cybersecurity Policies**.
4) Anticipate and remediate process and system Deltas/Problems before they fail.
5) Exploit the organization's Strengths/ Advantages to build cohesive and creative responses across the enterprise.
6) Create a robust **Action Plan** to remedy Deltas or improve the Cybersecurity capability through a highly integrated team implementation. Remediation or improvements may include: updated Cybersecurity policy, process or plan redesign, creative user alerts, innovative Staffing, and the required technology upgrades.

The ACAP process is then iterated in 1-6 month cycles, much like the Agile Development's "Sprints" process, each session building on previous ones. Timing of the cycles depends on the organization's Threat Tempo. ACAP sessions can also be held outside of the planned iterative cycles, if dictated by Emergent Threat technology advances or other events.

1.1 The Newly-Mandated Compliance Culture

The President has directed the following agencies to put out coordinating US policy on Cybersecurity:

GOVERNING AGENCY	SPHERE OF GUIDANCE
Office of Management and Budget (OMB)	Memo 14-13: Mandates Information System Continuous Monitoring (ISCM)
The National Institute of Standards and Technology (NIST)	Special Publication 800.53 Rev 4 and now 800.137 provide broad framework for National Cybersecurity Standards
Department of Homeland Security (DHS) – Continuous Diagnostics and Monitoring (CDM) and Continuous Monitoring as a Service (CMaaS)	Funding and Acquisition Vehicles for Automated Monitoring Cybersecurity Tools and Processes

The NIST Special Publication 800-53, Revision 4, ***"Security and Privacy Controls for Federal Information Systems and Organization,"*** is the source of an integrated set of security protocols and guidelines for Federal Agencies to respond to a wide range of attacks "including hostile cyber attacks, natural disasters, Structural failures, and human errors." NIST 800-53, Rev 4, specifies the hundreds of tools and processes needed for developing a holistic approach to Cybersecurity.

Ironically, the ACAP process may actually support and galvanize the new Federal Cybersecurity Framework. The Framework is a breakthrough in many respects – its sourcing in NIST itself, brings a level of rigor and credibility to the effort; offers a common Cyber language across organizations; establishes groundwork for future evolution to strengthen Cyber protections over time; uses a window of risk assessment and management, and leverages a continuous improvement process, a hallmark of sound Federal operations.

Nevertheless, the Framework adoption is currently voluntary and adoption has been slow. Since the origins were not based on Congressional input, the Framework does not have the force of law. The Administration is in the process of working with government and industry to devise meaningful incentives. At the same time – as one commentator noted – this Framework is not laboring under a pretense of being a "Cyber 400-level course." There is somewhat widespread agreement in the Cyber community that the Framework, albeit an advance, has serious gaps and will need adaptive, creative thinking to be fully operational.

1.2 The Drawbacks of a Cybersecurity Compliance Culture

The main flaw in a Compliance Culture is the belief that compliance activity leads to security. It may, but more often reliance on compliance alone produces a false sense of security. Ironically, relying on a compliance model alone may also give Cyber adversaries the current Cyber playbook and strategy. There is an additional risk in sending out compliance documents or updates to the regulating organization, or even holding them on the network/system, may inform adversaries about vulnerabilities.

Unfortunately, the typical response to more Cybersecurity challenges is to reach for narrow technology fixes and compliance doctrine, rather than step back and take a Strategic, cultural, holistic, and knowledge/ human intelligence-based approach. These heretofore under-utilized competencies are the critical success factors essential to competent, rapid, and adaptive responses in this relatively uncharted world of emerging Cyber-threats.

The problem is that the "Cyber Barbarians at the Gate"-- whether state or non-state actors, criminals or hacktivists -- are constantly looking for front gates, back doors and chinks in the castle mortar. Cyber-attackers are disturbingly creative and adaptive in use of social engineering to gain access. Threats are multi-variant: Cyber-attackers are as different in their methods, as in their origins, and their methods are constantly evolving. So no matter how good one's processes and technology are, they will adapt around them. The more static and compliance-focused one is, the easier it is for them to get around efforts to contain them.

U.S. Cybersecurity organizations are additionally hindered by budgetary and bureaucratic stipulations, and a culture that limits smart knowledge-gathering, information-sharing, and adaptive response. The often very adaptive Cyber-attackers, on the other hand, are advantaged in they are required to only bat .001, while Cyber-defenders have to bat 1.000. The cyber "offensive technology" refresh cycle is generally easier and more rapid than the typical "defensive technology" refresh cycle.

With all best intentions, without changing the Cybersecurity culture, the new Federal Cybersecurity Framework could leave our IT systems as -- or more -- vulnerable than before, because the existing "compliance culture" will make compliance to the Framework the measure of success. This may leave our systems unshielded in the face of adaptive and creative intrusions.

Another problem is that compliance activity is very time consuming. Added to that, the Cybersecurity operational tempo is uncertain, rapid, varying, and with unforeseeable sudden changes, which just makes it difficult to thoughtfully plan strategically, review policies and coordinate ongoing remediation, actions and upgrades.

1.3 How ACAP Creates an Adaptive Cybersecurity Culture

So how can ACAP make a significant impact in Cybersecurity culture and the challenges faced in Cybersecurity? First of all: Culture and strategy necessarily inform each other. How an organization reacts to or anticipates threats -- including Cyber – reflects organizational culture. How leaders make Cybersecurity strategy decisions reflects the leadership culture. How ready technical staff and stakeholders are to adopt new courses of action reflects worker culture. The organization that can effectively tackle the nuanced, sophisticated and adaptive Cyberthreats requires an active, vibrant, interactive culture.

There is an inherent tension between the classic tendency to resist information-sharing in order to protect, and the need for rich exchange of information required for success in Cyber strategy. Effective culture change means weaving technical staff and stakeholders into the decision-making and implementation processes. New ideas on Cybersecurity strategies will emerge as information-sharing and shared problem-solving skills become the norm within the ACAP Strategic Team and across the organization.

An Adaptive Cybersecurity Culture to successfully take on Cyber challenges will also require:

1. Rapid Decision Making: ACAP eliminates endless PowerPoint presentations and management review cycles. The tempo of Cybersecurity today cannot afford long studies, reviews, extended comment periods and multiple levels of sign offs. The multi-level, cross-functional ACAP Strategy Team puts critical voices in the room so a cogent decision can be made in near real time.

2. Rapid Implementation: ACAP reduces the gap between decision and implementation. ACAP ensures that people instrumental to decisions help implement the ACAP Action/Implementation Plan. Formal and informal involvement of existing staff – rather than hiring new or consultant support -- provides more implementation throw-weight for leadership to use.

3. Treatment of Cyber Technology as An Integrated Portfolio: ACAP becomes a *de facto* Cybersecurity Technology and Project Portfolio Management decision-making process where need and context are part of the technical and process analysis. Portfolio Management creates decision rules to guide acquisition and project funding decisions. Savvy Portfolio scrutiny eliminates duplicative, rogue, or pet projects for a common Enterprise Architecture. The ACAP Strategy Team becomes the Cyber-Technology Portfolio Management group (or at least can provide the driving logic behind any current Portfolio Management Process).

4. Greater Coordination between Technology, Policy, and Budget:
The rapid assessment against current Threat /Risk Matrix aligns and targets technologies, processes, Staffing and policies to the current Cybersecurity needs. But it is critical that those decisions about changes in technology, process and policy are being made as integrated and cohesive set, by a cross-section of the of the Cybersecurity organization that includes C-Level participants. For example, changes in processes or technology will likely require changes in Cybersecurity policy.

5. Speed and Iteration: ACAP builds on the lessons learned from Agile Development: ***Try, Test, and Revise.*** While the current Federal Cybersecurity Framework Approach is much closer to the constraints of Requirements-based Development, ACAP leaves much more flexibility for innovation, adaptation, and testing of ideas.

Requirements-based Development has been seen as providing stable development. The incompleteness of Requirements Based Development has been shown that getting all requirements up front is really hard, very time consuming, and is often never complete, or conversely, just too complete. Agile Development grew out of the effort to model what really happens in development projects, and to avoid loss of large amounts of time and energy on developing requirements that end users never really wanted and missing other requirements that were unforeseen. Moreover, it is hard to change requirements, both practically and often contractually. Rigid requirements reduce adaptability to the changing environment.

6. Levels the Playing Field of Ideas through Dialogue: ACAP relies on Professional Master Facilitation to manage power disparities in the organization, and make sure that technologists don't just rubber stamp Leadership's ideas or that Leadership simply ignores technologist's warnings or solutions (or, sometimes, overly-rely on technologist advice in preference to good business or policy judgment). As a result of the ACAP dialogue, technologists may begin to understand some big picture issues and budget challenges associated with their recommendations. Leadership, too, become more insightful about technologist reasoning and recommendations.

Because decisions often must be made on incomplete technical or budget data, generating conversations that are trusted and respectful is valuable. A rich diversity of perspectives can fill in gaps in knowledge and insights. All voices must be able to challenge assumptions and create richer solution sets and scenarios.

7. Increases the Likelihood That Existing Undiscovered Breaches will be Discovered and Remediated: ACAP preparation requires system inventories and audits to make sure analysis is based on current system data. The net effect is that closer scrutiny and group analysis of the system by the ACAP Strategy Team can result in identifying hidden breaches.

8. Creates System and Organizational Learning: In the ACAP process, problems are not put in reports to hide as shelfware. Problems are front and center. A cross-section of the organization can see problems (and where possible, opportunities), learn from them, and identify new solutions. The ACAP process focuses on continuity of learning from experience and shared insights.

9. Builds in Organizational Resiliency: The ACAP Strategy Team is more likely to be resilient and responsive in the event of a significant negative event. Groups that have become high performing teams develop problem solving skills, shared insights, and more trust in their members. In the event of failure, this kind of high-performing team and organization will experience much less blaming and cover-up behavior than in a traditional fully-hierarchical organization. The ACAP Strategy Team can move with much quicker, more responsive problem solving.

2.0 About The Agile Cybersecurity Action Plan (ACAP): From Compliance Culture to Adaptive Culture

To accomplish this essential change, ACAP uses a hybrid approach integrating: Adaptive Strategic Planning, Risk Management, Agile Software Development and Planning, Stakeholder Engagement, Customer/User Outreach, and Network Operations Center Best Practices. ACAP is not an engineering model, but an approach to Cybersecurity Strategy that has some engineering aspects in it.

All Cybersecurity efforts entail a constant struggle between detail and speed. The ACAP Facilitation component will need to manage the dynamic tensions of big picture versus technical details, as well as the extremes of technical over-simplification or over-complication, which can lead the group into unending, and fruitless, discussions.

Cybersecurity Strategy must become an “Adaptive Strategy***.”*** Rather than a long-range document that is 95% fixed, Cyber-organizations need a new Adaptive Strategy that leaves room for the emergent and unforeseen. This Strategy may include Scenarios that anticipate, but do not lock down solutions for unplanned (the “unknown unknowns”) yet urgent conditions. Adaptive Strategy is often referred to as the “80% solution” – and may even be closer to a “65% solution.” James Lewis, Senior Fellow and Director of the Technology and Public Policy Program at SAIS, uses the term, “Wild, Wild West,” to describe the current turbulence and vulnerability of Cyberspace. The Agile Cybersecurity Action Plan must be even more resilient than previous compliance-based models, and guide leaders and key technical specialists to adapt rapidly in this changing and emergent threat environment.

The Federal Cybersecurity Framework has good starting points and supportive checklists, but ACAP provides the adaptability needed to deal with changing threats and changing Cybersecurity requirements.

Because ACAP is a strategy and action plan process and not a technology framework, it is ***“framework-agnostic.”*** In other words, the ACAP Process provides organizations the liberty to adapt and work readily with a wide range of more technical and detailed Cybersecurity process models (e.g. FISMA-DHS/NIST, SANS, ISO, etc.). ACAP can utilize whatever security controls standards that are place or that the organization wishes to switch to, or creates. There is no de-confliction needed in creating a solid baseline Cybersecurity checklist or strategy foundation.

3.0 The Agile Cybersecurity Action Plan Process: Readiness for Success

The core ACAP process is launched through a facilitated 1-3 day ACAP Strategy Team session held in a to-be-determined cycle. The initial session will likely be longer and may be broken up into segments a week or two apart. Much of the work of the ACAP Strategy Team is done in sub groups or tasked to Subject Matter Experts (SME), who then report to the full session of the ACAP ST.

The direction and structure of the Agile Cybersecurity Action Plan must be closely aligned to the organization’s Business Strategy and supporting Enterprise IT Strategy. So each ACAP will be unique to the specific organization in which it resides, yet have some common characteristics.

Key decision makers and lead technical specialists must think through the linkages from the overall Enterprise Strategy and Mission to the operational Agile Cybersecurity Action Plan. The intent of ACAP is to create an inclusive strategy that touches all aspects of the Cybersecurity strategic and operational planning, threat/risk mitigation, operational monitoring and incident response. While each iteration of ACAP may identify gaps and needs in the Cybersecurity process and infrastructure. The key is to focus on identifying initially solvable issues and then to actions to fix or mitigate these issues, while at the same time maintaining a grasp of any additional issues for resolution at a later time.

There are some best-practice-based Readiness conditions essential to support successful development of the ACAP process. These tasks are actually important for any sensitive, high-level, complex initiative. Especially, however, their absence in the volatile, unpredictable, ever-changing world of Cybersecurity could be definite Failure Factors.

3.1 Leader-Sponsorship and Enterprise Governance

As mentioned before, the most critical pre-requisite is **C-Level** (CIO, CSO, CTO or COO) **sponsorship** and **participation.** Without C-level participation, the speed of decision-making and implementation is lost. Moreover, absence of this level of leadership reinforces the hierarchical culture, which in turn reinforces a "compliance culture." People are willing to take more risks if they see leadership taking risks with them.

If there is no Enterprise IT Governance Structure (which is an IT best practice), this can be problematic. Without a Governance Process to focus on controlling major technology acquisition, technology changes, and major policy or Staffing changes, IT resources get nibbled away into rogue, vanity and pet IT projects.

But more critical is the alignment of ACAP with any existing IT Governance Structures. In theory ACAP leadership of IT Governance should be the same or peers. Building a Strong relationship between ACAP and any existing IT Governance Structure is a critical success factor. Failure to manage the leadership integration at this level can result in delay – or worse, divergence in leadership direction, and/or blocking of essential resources for changes and technology upgrades.

3.2 Operational Cybersecurity Command & Control

A lack of institutionalized Cyber Command and Control is a potential Failure Factor. Cybersecurity operation that cannot function effectively will hardly be able to move to the level of sophisticated, future-forward, adaptive management required for ACAP success. ACAP relies on participation of many levels of the IT/Cybersecurity leadership, so if there is lack of effective of command and control, this will impact ACAP's situational awareness, insight, and effectiveness in implementations.

3.3 Learning and Knowledge Management Infrastructure,

Organizations that don't learn from mistakes, are likely repeat them or a variation of the mistake. Learning from mistakes or successes is critical to success in the Cybersecurity realm. Organizations that lack any Knowledge Management (KM) Processes or Strategy are at disadvantage. So while there needs to be a separate Cyber Knowledge Management Strategy to maintain secure Cybersecurity insights, but this becomes more challenging when the organization has no KM processes in place. The extra work entailed in producing Cybersecurity Knowledge Management and, if there are no foundational plans to build on. But the lack of these lynchpins is another potential Failure Factor.

3.4 Strategic Communication Infrastructure Plans

Because so much of adversaries' Cybersecurity strategy is based gaining access through social engineering through "phishing" activities, Cybersecurity must rely on Strategic Communications (Strat Comm) to counter their social engineering. An organization that lacks Strat Comm infrastructure is also at a disadvantage. Developing effective Strat Comm is sometimes resisted because it is antithetical to the secrecy and security mindedness that tends to characterize Cybersecurity organizations.

4.0 8 Key ACAP Success Criteria: Out Thinking the Barbarians

The challenge, as mentioned before, is to be able to respond to the adaptiveness of the Cyber-barbarians, while managing the compliance culture and bureaucratic obstacles that slow responsiveness. Below are 8 success criteria for ACAP implementation:

4.1 Rapid Execution and Agile Process

The creation of an Agile Cybersecurity Action Plan must be executed rapidly, in several intense days (rather than the customary year-long Strategic Planning process). The horizon focus for an ACAP Portfolio must be no more than a year out. The ACAP Plan must be, at a minimum, reviewed and updated quarterly. The smartest "test review cycle" would be monthly or bi-monthly -- or as needed -- to ensure timely response to major emerging threats, Cyber actor(s), or technologies. ACAP is an agile process and is not about perfection; rather, provides "mighty good" and "getting better through iteration" results. The brevity of the process may in fact be good news to organizational decision makers with tight schedules: The process allows for getting the best minds in the room, working together with rapid efficiency, and moving on.

4.2 Senior Leadership Sponsorship and Participation

Without C-Level leadership's willingness to visibly sponsor ACAP, and commit some of their time and resources to the process, ACAP will produce marginally better results than current approaches. This is not the usual "throw over it the fence," hire consultants to write a report that will sit on the shelf so leaders can check it off as "done." This is ***doing*****.**

This may be a challenge for some leaders who are used to hiding out in the organization's hierarchical Structure and limiting their access to subordinates. This requires leaders to be somewhat accessible, at least around the ACAP process. More importantly, senior leaders need to come to the process ready to make decisions with the ACAP Strategy Team. This is not like many decision processes where subordinate Staff brief leaders who then go off and make decisions elsewhere. This is making decisions in a working "smart team" context.

4.3 Representative Participation

The ACAP Process is run by the **ACAP Strategy Team (ACAP Strategy Team).** This Team must have a defined membership, representing different levels of authority and a broad cross-section of Cybersecurity professionals. Participants must include key C–Level leaders, the organization's brightest technical minds, and members of the Governance Structure including the CIO, CTO, and CSO, as well as representatives of key Technical/ Strategy Working Groups, and SME's. This group may also include Stakeholder participants like "end users" who can provide additional insights. The ACAP Strategy Team must work at a high level of performance in collaboration, knowledge sharing, communications, and building rapid plans of action. The group must avoid "Groupthink" by embracing healthy dissension. Some variance in knowledge, points of view, and preferred courses of action can lead to smarter outcomes – provided the group has the skill sets to work through these dissensions.

4.4 Facilitated Process

For the ACAP Strategy Team to address honest dissension and put difficult issues on the table, collaborate at a high level, share knowledge, and move to rapid, responsive solutions requires a **Master Level Facilitator or Facilitation Team**, trained in the ACAP Process. This level of Master Facilitation expertise is a *sine qua non* to ensure the ACAP Strategy Team generates what Dorothy A. Leonard, Professor Emerita of Corporate Creativity at Harvard and MIT, calls *"creative abrasion"* -- best thinking, rapidly creation of solution scenarios for consideration, preventing the Team getting lost in the weeds of technical or policy details, managing dissension, and moving rapidly toward closure with best ideas. Not easy to do, hence the expertise required.

In other words, Leonard's concept of *creative abrasion -- the exploitation of intellectually diverse perspectives to foster innovation* – is essential. Breakthroughs can occur "when different ideas, perceptions, and ways of processing and judging information collide."

Readiness to explore and entertain a wide range of adaptive possibilities is a critical success factor for Cyber-organizations – as Leonard says: “putting your organization’s whole brain to work.”

4.5 Use of Subgroups

Much of the work of the ACAP can and should be done in Subgroups working on specific issues or policies, and then brought back to the ACAP Strategy Team for final decision. This will make Team sessions much more productive. Subgroups may also provide additional research and option development in advance of Strategy Team sessions.

4.6 Encouragement of Culture Change

Inherent and vital to the success of the ACAP process is creation of an Adaptive Organizational Culture – valuing change, “early-alert” systems, good ideas, and incorporating diversity in thinking and perspective, versus static and conventional bureaucratic approaches.

Therefore, a key player in the ACAP process to achieve culture change must be an **Organizational Change Management (OCM) Expert.** Those who have tried substantial culture change will understand that response to changing conditions only happens well with skilled OCM guidance. A fully comprehensive OCM Plan, coupled with organization-wide technology and process adoption, are the success factors here. Necessary culture change approaches very likely will be at odds with a “compliance-focused” Cybersecurity organization, and thus require developing a sophisticated valuing of adaptive Strategy over legacy rigid bureaucratic habits.

4.7 Action Planning

ACAP is focused on Action Planning and has a distinct bias for doing -- versus just writing attractive reports and shelf-ware. The Action Planning component is a dynamic guidance document, but it will be the ACAP Strategy Team members who step up and take on leadership roles that spur successful Cybersecurity outcomes. As new action elements are identified, rapid delegation and implementation are followed up with attentive scrutiny. Timeframes for each level of action are stipulated and monitored.

4.8 Use of Subject Matter Experts (SMEs) with the ACAP Strategy Team

Skills and expertise often overlooked in substantive Organizational and Culture Change are essential for ACAP success. Two of these have been discussed already:

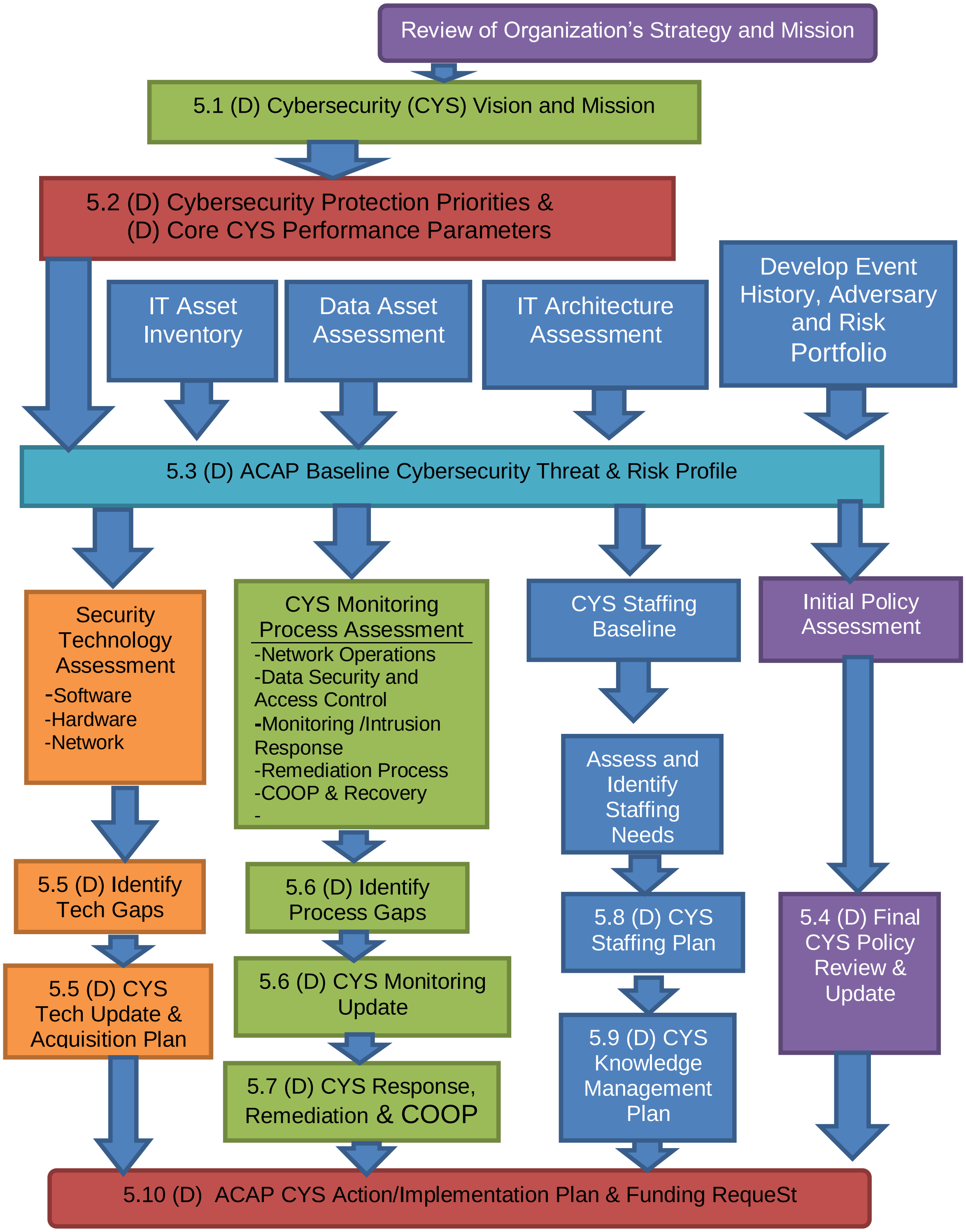
- **Master Strategy Team Facilitator (Section 4.4)**
- **Organizational Change Management Expert (Section 4.6)**

In addition, these three additional areas of expertise should be added:

- **Threat/Risk Management Planning Specialist(s):** To guide the work of the Agile Enterprise, these specialists must be adept at building plans that are unusually fluid, environmentally-scanning, and capable of generating “blue-sky” Threat/Risk thinking among contributors across the enterprise
- **Penetration Testers:** External “Extreme Hackers” who engage in “White Hat Penetration Tests” can provide sobering and useful insights to the ACAP Process. Penetration Testers can participate on a part-time basis.
- **Attorney-Advisors:** In some unique situations, having legal advice ready at hand and familiar with the Team’s issues could prove very valuable, particularly in cases of issues of privacy or Personally Identifiable Information (PII).

5.0 Creating an Agile Cybersecurity Action Plan

Flowchart of Steps and Deliverables to Develop ACAP


Review of Organization's Strategy and Mission
5.1 (D) Cybersecurity (CYS) Vision and Mission
5.2 (D) Cybersecurity Protection Priorities & (D) Core CYS Performance Parameters
IT Asset Inventory
Data Asset Assessment
IT Architecture Assessment
Develop Event History, Adversary and Risk Portfolio
5.3 (D) ACAP Baseline Cybersecurity Threat & Risk Profile
Security Technology Assessment
-Software
-Hardware
-Network
CYS Monitoring Process Assessment
-Network Operations
-Data Security and Access Control
-Monitoring /Intrusion Response
-Remediation Process
-COOP & Recovery
-
CYS Staffing Baseline
Initial Policy Assessment
Assess and Identify Staffing Needs
5.5 (D) Identify Tech Gaps
5.6 (D) Identify Process Gaps
5.8 (D) CYS Staffing Plan
5.4 (D) Final CYS Policy Review & Update
5.5 (D) CYS Tech Update & Acquisition Plan
5.6 (D) CYS Monitoring Update
5.9 (D) CYS Knowledge Management Plan
5.7 (D) CYS Response, Remediation & COOP
5.10 (D) ACAP CYS Action/Implementation Plan & Funding RequeSt

© 2015 John W. Link & Jo Lee Loveland Link

(D) = Deliverable

Integrated Steps and Deliverables for ACAP

After the basic prerequisites have been met and appropriate leader sponsorship is on board with the ACAP process, ACAP can begin in earnest, with these elements:

Data Collection for Strategic Insight:

- **Internal data** about the system and elements on it, Executive Leadership's Strategy for the organization, history of Cyber intrusions, and enhanced organizational capacities.
- **External data** about emerging threats, adversarial adaptiveness, shifting global political alliances, technology trends, and emerging methodologies of social engineering.

Plan Steps and Deliverables: Streamlined and as simple as possible, but deliverables must be integrated, iterative, emergent, that change and mature over time, as shown in the following chart.

Chart of Integrated Steps and Deliverables for ACAP

Deliverable 5.1 Defined Cybersecurity Vision & Mission
Deliverable 5.2 Identified Cybersecurity Protection Priorities & Performance Parameters
Deliverable 5.3 Baseline Cybersecurity Risk and Threat Profile
Deliverable 5.4 Cybersecurity Policy Review and Update
Deliverable 5.5.Cybersecurity Technology Update and Acquisition Strategy
Deliverable 5.6 Cybersecurity Continuous Monitoring Plan Update
Deliverable 5.7 Cybersecurity Response, Remediation and Continuity of Operations (COOP) Strategy
Deliverable 5.8 Cybersecurity Staff Assessment and Staffing Plan
Deliverable 5.9 Cybersecurity Knowledge Management Plan
Deliverable 5.10 ACAP Implementation and Action Plan & Funding Request
Review and Update Regularly

Below are explanations of each of the deliverables:

5.1 Define Cybersecurity Mission & Vision

The ACAP Strategy Team needs to use the organization's existing Strategic Plan as Starting point for the development and alignment with the Cybersecurity Vision and Mission. Participants in such a high-velocity, high-sensitivity efforts as ACAP, usually have very divergent ideas about what matters most to the organization. Forging these divergent ideas into a cohesive Cybersecurity Vision and Mission, if well-handled, can be a valuable output of the ACAP Strategy Team. Resolving frictions and merging these disparate ideas can result in new and highly useful insights for the organization's Cyber protection.

5.2 Identify Protection Priorities and Performance Parameters

Participants will use existing organizational Strategic Plans and guidance to develop the protection priorities and performance parameters**.**

5.2.1. Define the Protection Priorities- Decisions will have to be made regarding best use of limited resources. These decisions will need to be made with firm resolve to implement in a crisis.

5.2.2. Define Level of Cybersecurity Performance Parameters – "Deep dive" insightful questions must be answered regarding achievable Cybersecurity performance. These questions must include (but are not limited to):

- What part of the Cybersecurity system is most vulnerable to risk?
- Which are most imperative priorities to maintain?
- What is the maximum downtime permissible for ongoing operations?
- Is the expectation that the system will never/ seldom be penetrated?
- If so, what changes in thinking need to be remedied across the organization? What determine that? Who decides?
- How resistant to phishing activities are the end users?
- Given a certain amount of risk tolerance, what changes in thinking need to be remedied across the organization?

5.3 Develop the ACAP Baseline Cybersecurity Threat and Risk Profile

Much of the research in creating the Baseline Cybersecurity Threat and Risk Profile may be done in advance of the ACAP Strategy Team Session. The Baseline document may be developed as a first draft in the initial session. The ACAP Strategy Team then updates this draft with pre-session research and additional group inputs in subsequent sessions.

5.3.1 IT Asset Inventory

Identify all the IT assets on the system. Asset analysis will need to be broken down into a useful taxonomy and the IT assets inventoried for analysis. This is followed by development of an IT inventory asset updating process.

5.3.2 Data Asset Assessment

Identify the System's databases and prioritize their vulnerability, value, and sensitivity.

5.3.3 IT Architecture Assessment

It is critical to have a current and accurate System Architecture so that any architecture structural cybersecurity problems can be identified and managed.

5.3.4 Develop Event History, Adversary and Risk Portfolio

A key area of analysis is to create an ***Adversary and Risk Portfolio,*** which includes:

- History of significant intrusions and near-successful attempts
- All currently identifiable threats and sometimes even remote threat possibilities
- Careful analysis of sources, causes, likely evolution, etc. in the threats

To create an Adversary and Risk Portfolio, the ACAP Strategy Team (or designated Risk Subgroup) tracks adversary history, emerging adversaries, non-adversary risks, and emerging open and "underground" technology developments.

5.3.5 Structure a Threat and Risk Management Matrix to Examine Probabilities and Impacts

The next Step is to put the Adversary and Risk Portfolio into in ***Threat and Risk Management Matrix*** below. Each threat and risk will need to be analyzed for potential ***Probability*** and ***Impact*** (Fig. 2)

Fig. 2 Threat and Risk Management Matrix

	High Impact	Low Impact
High Probability	High Probability High Impact	High Probability Low Impact
Low Probability	Low Probability High Impact	Low Probability Low Impact

Threats/Risks may shift location in the Matrix over time

The ACAP Strategy Team (or a Subgroup) will need to identify both known risk elements and include "unknown unknowns" or "incipient"/ "fuzzy risks" that have not fully emerged yet, but pose high levels of risk if they do occur. Examples: Quantum computing is an example of an incipient risk that may make password security obsolete, but which is currently limited in availability. Underground technology development is an "unknown unknown" risk.

5.3.6 Conduct Threat/ Risk Assessment and Mitigation Planning for Priority Risks

Each of these quadrants will likely require different kinds of attention: e.g. Threat/ risks that are "Low Probability/ High Impact" entail generating an array of multiple scenarios and contingency plans for unpredictable situations. Whereas, by contrast, threat/risks that are "High Probability/ Low Impact" may well be able to draw on tried-and-true former solutions for sufficient readiness.

This work is often very challenging to groups. Adding an accomplished, experienced **Threat /Risk Management Specialist** to the ACAP Team can be very helpful to take risk management to levels that are efficient, effective, doable, and reach across the breadth of Cyber-threats. A sound and inclusive ***Threat/Risk Management Process*** is another critical success factor in Cybersecurity. Cyber-analysis is working to see around the dark corners: risk management can accelerate these efforts.

The ACAP Strategy Team will finalize the ***5.3 Baseline Cybersecurity Threat and Risk Profile*** analyzing identified top priority risks against Cybersecurity Protection Priorities, the Cybersecurity Performance Parameters, and the broad Asset Inventory and Architecture Assessment to create a holistic threat/risk profile of the Cyber system.

5.4 Cybersecurity Policy Review and Update

This step has an initial review of Cybersecurity Policies. Only after the group has completed the Threat and Risk Profile will a policy review be meaningful. Policies need to balance current user needs with emerging risks to operations and security.

After the various plans that make up the ACAP have been developed, an additional Cybersecurity Policy review of the proposed process and technology plans is needed to ensure that any recommended changes will synch. Policy review and updates are needed to define behaviors and processes to respond to identified risks.

5.5 Cybersecurity Technology Update and Acquisition Strategy

The ACAP Strategy Team can use existing or create its own Technology Categories for analysis. Here an example of a very rough set of potential categories for Technology Analysis and some example technologies that might fit in the category.

1. **General System Monitoring-** Applications for monitoring the general State and health of the network, which can provide useful diagnostic data. Examples: *Paessiers (PRTG), CACTI, and Spiceworks*

2. **Cybersecurity Monitoring –** Applications used for detecting intrusion. Examples: *HP's Arcsight, Dell's Secure Works, NMAPP, Syslog-NG, After Glow, Fire Eye, Mandiant and Juniper FW*

3. **Visualization, Analysis and Management**
Examples: *CyVision's Cauldron, VNMAP, Red Seal, SkyBox, NetSpa and Splunk, Avert, and Visual Analytics*

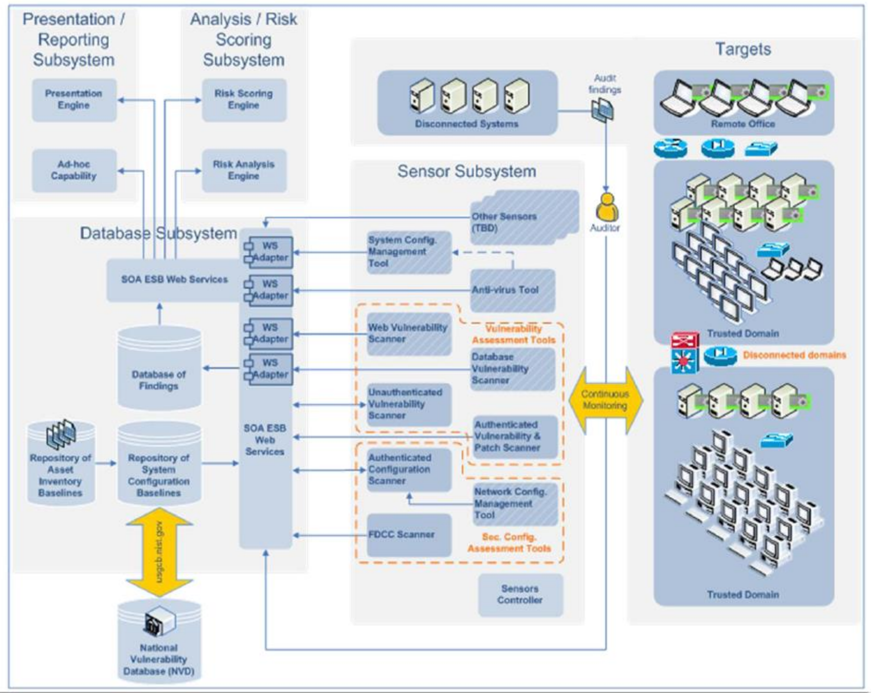
4. **Remediation Applications:** This includes a range of software to fix applications and other software. Examples: *IBM Appscan or Kaspersky Labs Suites*

5. **Remediation Project Management:** Helps to manage the Staffing and logistics of the Remediation Effort. Example: *PRI's Cyber Action Suite*.

Because ACAP is "framework-agnostic," if an organization is already using the existing technology framework such as the Federal Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) reference model that can be used as the technology assessment framework. (See Fig. 3 below)

Fig.3 Federal Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture

Figure ES-1. Contextual Description of the CAESARS System


Presentation / Reporting Subsystem
Presentation Engine
Ad-hoc Capability
Analysis / Risk Scoring Subsystem
Risk Scoring Engine
Risk Analysis Engine
Database Subsystem
SOA ESB Web Services
WS Adapter
WS Adapter
WS Adapter
WS Adapter
Database of Findings
Repository of Asset Inventory Baselines
Repository of System Configuration Baselines
SOA ESB Web Services
usgcb.nist.gov
National Vulnerability Database (NVD)
Disconnected Systems
Audit findings
Auditor
Sensor Subsystem
Other Sensors (TBD)
System Config. Management Tool
Anti-virus Tool
Web Vulnerability Scanner
Vulnerability Assessment Tools
Database Vulnerability Scanner
Unauthenticated Vulnerability Scanner
Authenticated Vulnerability & Patch Scanner
Authenticated Configuration Scanner
Network Config. Management Tool
FDCC Scanner
Sec. Config. Assessment Tools
Sensors Controller
Continuous Monitoring
Targets
Remote Office
Trusted Domain
Disconnected domains
Trusted Domain

Source: Peter Mell, based on NIST IR 7756, jointly developed by DHS and NIST with NSA participation

Be aware that increased threats and changes to the Enterprise Architecture will necessitate changes to Cybersecurity technology needs. There may be other classes or groupings of technology that the ACAP Strategy Team may wish to consider and analyze to identify technology capability gaps or new classes of threats, which must have a technical countermeasure.

5.5.1. Finalize the Cyber Technology Refresh Strategy to Meet New Risks
With current technologies now in the new technology typology, the ACAP Strategy Team will identify any technology gaps. The next Step is to identify candidate technology for monitoring and remediation sufficient to respond to the newly developed Baseline Cybersecurity Threat and Risk Profile.

5.5.2. Develop a Cybersecurity Technology Update and Acquisition Plan to meet those gaps and emerging threats. This will generally fall into three classes that will inform tradeoff decisions:

1. **Must-Have Technologies & Updates**
2. **Should-Have Technologies**
3. **Would like-to-have Technologies (but not necessarily now).**

5.6 Cybersecurity Continuous Monitoring Plan Update

Cybersecurity Continuous Monitoring is a combination of sensor and monitoring activity to insure the ***Cyber Ecology*** is clear and functioning well enough to prevent Cybersecurity failure. Cyber Ecology includes: Organizational Mission + Architecture + Human Intelligence Assets (including the extensive network of social and business relationships including customers, partners and vendors) + Technological Assets.

5.6.1. Assess Network Operations Protocols

Sharpen the parameters of whom and what belongs or doesn’t belong on the system or network and the policies and processes needed to discern this. This must be extended to include: Asset Inventory, Human Resources Updates and related Social Networks.

5.6.2 Assess Data Security and Access Control Process

Where is the hierarchy of data located within the system, how easily can it be gotten to and what kind of access controls are there in place (Role Based, Clearances, Geospatial or Identity)?

5.6.3 Create/update the Organization’s Cybersecurity Monitoring and Initiation of the Response Processes

Identify gaps in the current monitoring processes and develop the Strategies and protocols to eliminate any monitoring process gaps. Next the initiation of response protocols needs to be assessed for process gaps that can be fixed.

5.7 Cybersecurity Response, Remediation and Continuity of Operations (COOP) Strategy

Critical to the ACAP Cybersecurity Strategy is clearly defining how to manage both General (Non-Crisis) Remediation and Urgent Incident Response.

5.7.1. General Cybersecurity Remediation

Identification of and remediation of vulnerabilities is a core business with the best ROI of almost any activity. It is critical to ensure that the general vulnerability remediation process is efficient, targeted and simplified.

5.7.2. Risk Reporting

The Cybersecurity Team in an organization will constantly be confronted with new data, insights and experiences that will highlight new risks to the System. Most organizations have some kind of risk reporting process and system. If there is not, one needs to be created by the ACAP Strategy Team.

5.7.3. Urgent Incident Response Preparation

Cyber Response needs to have lots of basic communication information, non-network communication to the organization, clear lines of authority, roles and responsibilities, targeted training and exercises. How will these remediation needs be triaged? These questions must be asked and answered: Is this process integrated with the Continuity of Operations (COOP) and Recovery Plans? Is information necessary to each part of the organization – or the entire Enterprise – known where needed? What gaps and training needs exist, and where? The ACAP process can help identify the kinds of processes and training needs of the organization.

5.7.4. Check the Monitoring and Response Plans against the Baseline Cybersecurity Threat and Risk Profile

The integrated Cybersecurity Monitoring Plan and Cybersecurity Response and Remediation Strategy will need to be validated against Baseline Cybersecurity Threat and Risk Profile to verify all the high to moderate risks are addressed.

5.8 Cybersecurity Staff Assessment and Staffing Plan

Changes in the ACAP may reduce or increase demands for personnel, as well as impact the level of skills and training needed to implement the new technologies or processes.

The Staffing Plan must baseline staff numbers and competencies to assess against numbers of staff needed for sound Cybersecurity operations in the context of the new emerging threats. This may be a guidance document that management may wish to use for final hiring decisions.

5.9 Cybersecurity Knowledge Management Plan

Creation and updating of the Staffing Plan will identify competencies and many cases additional knowledge required for the Cybersecurity Team to function under extreme operational conditions. The Cybersecurity Knowledge Management Plan and systems will be critical to making sure that hyper-secure Cybersecurity Knowledge Management Resources are not available to cyber adversaries, which might provide them dangerous vulnerability and protocol insights.

5.10 ACAP Action/Implementation Plan & Funding Request

The ACAP Strategy Team ensures that follow-up actions are prioritized and given adequate oversight. Implementation also provides an opportunity to reinforce the new adaptive cultural norms by having small teams implement changes and follow-ups.

Once technology gaps and optimum technology candidates are identified and priced/ budgeted to meet the Baseline Cybersecurity Threat and Risk Profile, the next Step is to initiate acquisition is to create and deliver a compelling funding request for sign off in either existing IT Governance or the appropriate C-Level Authority.

6.0 Begin the Iterative Process

6.1. Iteration and Versioning

Each of the iterations of the process is like an agile “sprint” that learns from each previous cycle and adapts to the evolving cyber threats and risks. This requires a clear ACAP versioning protocol, with a review and refinement process. ACAP is not “Strategic Shelfware” but a living, organic, operational guide with some Strategic elements. The current ACAP version needs to be given to all critical IT Staff, specialists, and organizational leaders.

6.2. Create an Ongoing Process to Ensure a Constant State of Readiness

This approach is about using iteration versus creating perfection. Schedule the next review session and subsequent sessions in a proposed frequency of review. There will be controls or issues that have not been fully addressed, and that is what the next session is there to do. The minimum requirement for an ACAP update is semi-annually, and the optimum update cycle is in terms of 1, 2 or 3 month cycles depending on the volatility of the cyber environment (or as needed). Once the ACAP is established, regular reviews and updates take much less time.

6.3. “Break-Glass Procedures”

In case of urgent incidents/ emergent conditions that reveal significant flaws in the current approach, there needs to be defined criteria and an agreed-upon process and timeframe to initiate, in near real-time, an emergency review and fixes for the ACAP.

Conclusion

The Agile Cybersecurity Action Plan (ACAP) creates a process for rapid ongoing revision of an organization's Cybersecurity Strategy on an iterative basis. This Strategy is based on an ongoing assessment the organizations unique Threat and Risk Profile against their Cybersecurity Technology, Processes, Policies and Staff. This process of analysis and strategy development is led by the ACAP Strategy Team that brings a cross section of organizational levels and expertise into the room in a facilitated process. This process moves between "Big-picture" Cyber-Strategy and the required technical engineering. The Cybersecurity Strategy is implemented by ACAP Strategy Team as part of the "Action Plan."

The ACAP process lays the foundation for an Adaptive Cybersecurity Culture that values collaborative problem solving, information sharing and action among people across the organization. ACAP embeds widely-shared knowledge and inculcates understandings that reinforce successful joint efforts for continuously emerging complex challenges. The ACAP process can radically improve the Cybersecurity posture of an organization, but will require commitment by a disciplined Senior Leadership to invest the time, key players, resources, policies, and communications for the necessary Adaptive Cybersecurity culture to take hold. Building a successful ACAP is not for the faint of heart – but is the most likely approach to build necessary strong safeguards in today's world.

John and Jo Lee are masters of the "human stuff," providing organizational management, communications and strategic consulting to corporate, government (DOD and IC) and non-profit clients. Jo Lee was for several years Visiting Scientist at Software Engineering Institute working with CMMI, Risk Management and Managing Technology Change at NRO, Warner-Robins AFB, and other agencies. John has worked for the Army Chief of Staff for Installation Management CIO, FEMA, DOJ, and others. Both were Senior Members of the Governance Team for the DOD OSD CIO/NII Horizontal Portfolio Initiative, one of the first demonstrations of cloud-based Information-sharing initiatives in DOD/IC. They have worked with Lucent, Johnson & Johnson, ARINC, and George Mason University, and nonprofit associations. They are co-designers/presenters for CHAOS, Inc. ™, an original experiential learning laboratory and seminar.

Please contact with feedback, inquiries or questions:
John Link and Jo Loveland Link
www.volvoxinc.com
johnwlink@hotmail.com
540-465-1491