Pathfinder Initiative - Concept of Operations

Rick Dove

by Rick Dove, rkdove@AgileSecurityForum.com
Agile Security Forum, www.AgileSecurityForum.com

Introduction and Values

The lack of a general strategy for information security within organizations, and the critical mismatch between security approaches and the real security environment was outlined in "Rectifying The Information Security Gap" [1]. That paper established seven areas of operating reality generally ignored in security policy, procedure, and practice.

This document outlines a Pathfinder Initiative that will illuminate the nature of this mismatch and understand how it impacts real operating environments; and from this new knowledge, will develop a fitness profile for rational policy, procedure, and practice. The Initiative will be conducted by a Pathfinder Group, consisting of participants from a representative industrial cross section of organizations who are concerned with the effectiveness of information security - both as users and as developers. The intention is a broad focus across the spectrum of information security policy, procedure and practice, not just the technology and service components that implement infrastructure and protection.

The knowledge and fitness profile developed in the Initiative will benefit the Pathfinder Group participants directly. They will develop a first hand understanding of how and why current practices are ineffective, and how they can be rationalized. Benefit accrues to the participants immediately by using this new knowledge to improve their policies and procedures, and the practices under their control. Some practice improvements must necessarily await action by the development community. In this later area, however, participants gain immediate value from a defined fitness path that guides acquisition of products and services, and accelerates development of conforming products and services. Additional important value comes from the geneses of an enlightened partner community - resulting directly from Pathfinder Initiative objectives that include the creation of a broad community wake-up-call and roadmap for compelling action.

To state the obvious, the frequency of security failures and the impact on productivity is reduced immediately as policies, procedures and practices become rationally aligned with reality; which reduces associated financial costs as well as the impact on organizational viability and trust. On the flip side, costs and impact will continue to increase by ignoring the realities of human behavior, organizational behavior, technology pace and complexity, globalization, and the increasing agility of both business practices and the attack community. What is the cost of even one publicized breech that shouldn't have been enabled?

Metaphorically Speaking

As intelligent, earth-walking, air breathers we can objectively observe and marvel at the fundamental rules and nature of the life-supporting aquatic world. Fish move gracefully in three dimensions - something we can't experience until the dreamed-of hot-rod hover-pack arrives. Synchronized wiggling propels them through their environment; a faultless choreography of three dimensional muscle control. Every body surface alternates at pushing against the surrounding water or slicing through it effortlessly. Specialized fins and tails evolved for speed and agility, and some with ballast sacs for float control. An infinite variety of shapes, sizes, and fueling needs; yet none is free of water-life reality. Though some enjoy brief soaring moments in the world of air, the reality of their environment and the reality of their nature limits what they can do, regardless of their dreams.

So it is with human organizations in social interaction. And like the fish, our reality is an unchangeable given. Both accommodated and leveraged. Unthinkingly. Unsensed. Ignored.

But unlike the fish, we have intelligence and unbounded aspirations. The two together have us fighting reality to soar in the ideal. It is the way we are wired. A constrained dream, nevertheless. But we can, in moments of studied reflection, separate idyllic aspirations from intelligence, make objective observation, and come to understand the limits imposed by reality. An honest moment. A rude awakening. An insight that can channel and leverage effort in concert with reality.

The Pathfinder Group will chart the nature of reality governing the world of information security, noting both the limits it imposes and the channels for mitigation and compatible synergy.

Mission and Participation

The mission of the Pathfinder Initiative has two parts:

1) To understand and articulate a rational general strategy for information security - resulting principally from knowledge discovery activities of the Pathfinder Group participants.

2) To cause a greater-community appreciation of that strategy and enable its pursuit - resulting principally from supporting activities of Forum staff.

Organizations participating in the Pathfinder Group will be involved in nine 2-½-day workshops that rotate among nine of the organizations. Host sites will be selected for the applicability of issues that can be analyzed and opportunities for solution profiling. Multiple participants from each organization will select participation in those workshops which focus on their personal areas of responsibility and interest, enabling a target completion of the workshop series in nine months. Published documents suitable for broad distribution and greater-community understanding of the knowledge development is anticipated to take an additional 2 months. The first workshop in the series will begin shortly after a minimum of ten Pathfinder organizations have made commitment of participants and costs. Cost to participate as a Pathfinder organization include a flat participation fee plus whatever travel expenses are incurred for sending participants to workshops. If an organization hosts a workshop they will incur some additional typical expenses associated with such an event. Participants will develop a visceral and actionable understanding of the issues and solution paths, and hosts will have the added benefit of collaborative attention focused on critical issues and opportunities.

The Agile Security Forum will provide planning, logistics, workshop facilitation, and management sufficient to achieve mission success. Knowledge developed by the Pathfinder Group will achieve the first mission element. Packaging that knowledge and promoting its compelling value with a greater-community involvement plan will achieve the second mission element. Based on earlier experience with the Agility Forum in the nineties, it is anticipated that a second phase initiative of greater community involvement will be enabled; and will be facilitated by an agenda of focus issues and a refined knowledge framework that emerges from the Pathfinder Initiative deliverables.

The principle activity of Pathfinder Participants is guided knowledge discovery. Meaningful and actionable knowledge is ensured by involving responsible decision makers and decision implementers. The breadth of necessary knowledge will rightfully span a broad range of organization functions, with representation as appropriate from CFO, CSO, CIO, CTO, HR, Product Management, Market Planning, Strategic Planning, and Risk Management areas. Real people with real problems. Real problems with current real-time criticality.

The Pathfinder Group will consist principally of participants from both user and developer communities. Whether these two communities are intermingled in a single track of workshops or meet in segregated parallel workshops is a decision

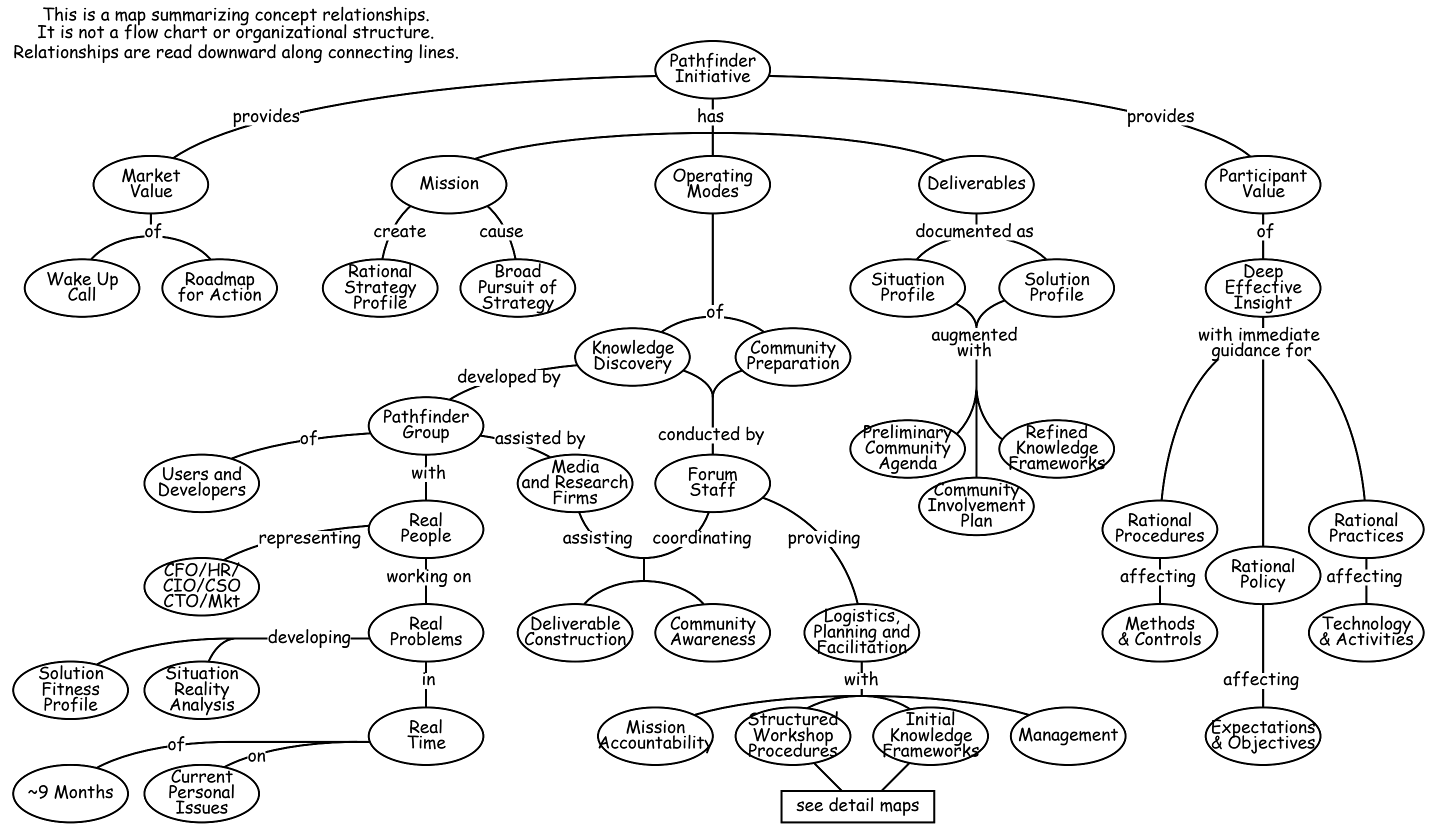

This is a map summarizing concept relationships.
It is not a flow chart or organizational structure.
Relationships are read downward along connecting lines.

Figure 1 – Pathfinder Initiative – Concepts of Operations

for the initial committed participants, as there are distinctly different twists on the issues for analysis.

The Pathfinder group will also include invited members from relevant trade media and relevant research and consulting firms. These will function primarily as observers, assisting Agile Security Forum staff in development of documentation deliverables and greater-community awareness.

It is recognized that workshop collaboration may deal with sensitive information. Participants will decide the necessity for non-disclosure agreements and what is permissible for inclusion in the deliverable documentation.

The operational concept is graphically summarized in Figure 1. Details on logistics and structured procedures, with a brief overview of knowledge development frameworks, follow.

Structured Workshop Procedures and Responsibilities

Structured workshop procedures are employed to ensure that objectives are met and that a body of consistent and high-quality knowledge is developed. These procedures build upon ones developed for successful similar cross-industry collaborative knowledge development in the nineties at both The National Center for Manufacturing Sciences and subsequently The Agility Forum.

Knowledge development will occur in a series of nine workshops. Workshops will each be 2-½ days in duration and occur as frequently as participants are willing to meet. Workshops will begin at 7:30am with a light breakfast in the workshop room, break for lunch and dinner, and include an evening break-out group exercise off-site following each of the first two workshop days. The third workshop day will end mid-day in time for return flights. The evening before the first workshop day will have a dinner session to break the ice and outline that workshop's objectives and procedures.

The first workshop is a kick-off session that will review objectives, the knowledge frameworks and procedures for workshop employment, logistics and schedules, and the candidates for analysis and solution exercises. The final workshop will review the knowledge development results, the document deliverables plan, the greater-community involvement plan, and a suggested greater-community focus agenda. The seven intervening discovery workshops will focus on the seven reality-issue categories, addressing two or three in each workshop to allow multiple perspectives.

The issue-focused discovery workshops will be organized around four prime activities: a review of preparatory reading material, analysis of host-provided issues, an exercise in solution profiling, and a performance review. Preparatory reading material will be sent in advance and chosen for relevance to the issues that will be analyzed. Two to three issues will be presented by host personnel and each will be analyzed according to initial frameworks discussed later, and refined

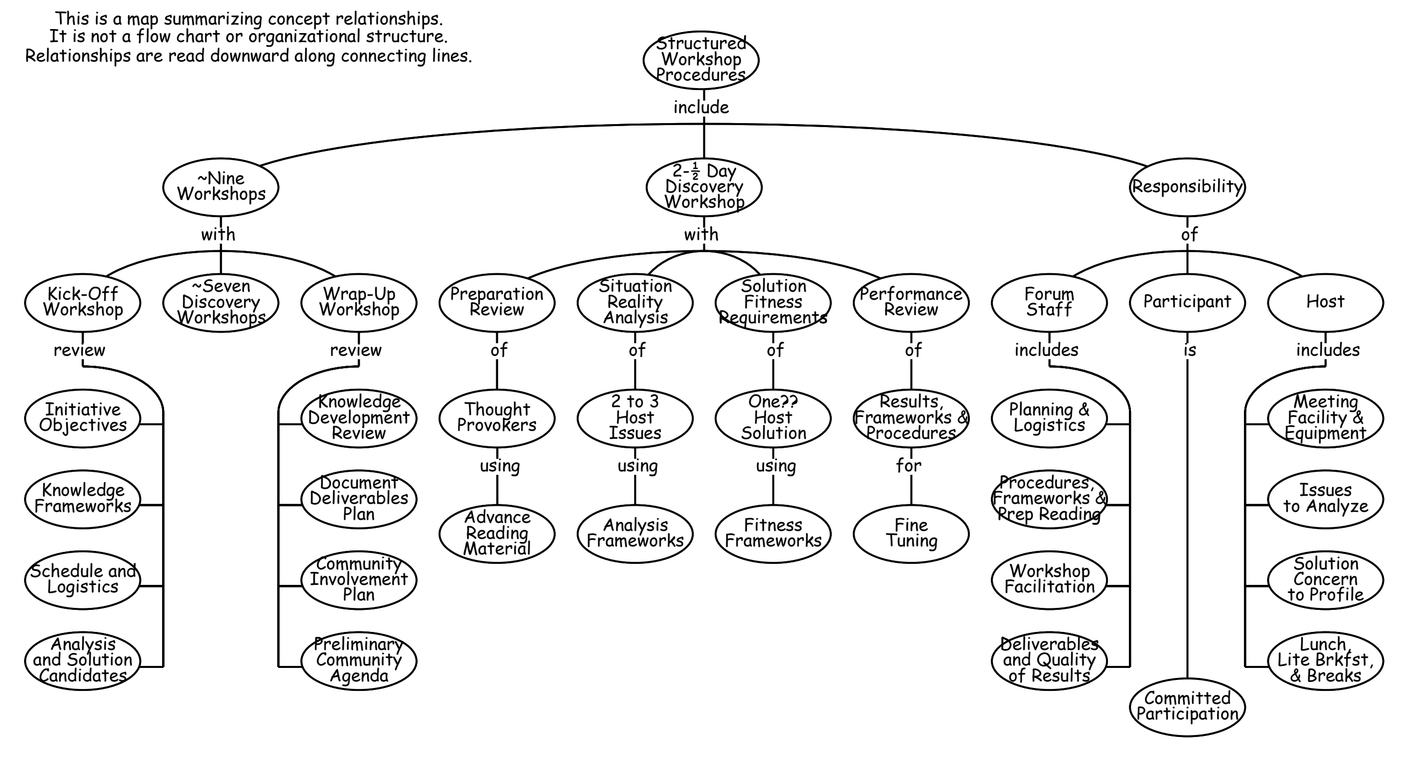

This is a map summarizing concept relationships.
It is not a flow chart or organizational structure.
Relationships are read downward along connecting lines.

Figure 2 – Pathfinder Initiative – Structured Workshop Procedures and Responsibilities

in practice by the Pathfinder Group. As time permits, a host provided problem will be profiled for solution fitness requirements compatible with the understandings that arise from issue analysis. The workshop will conclude with a review of procedures, frameworks, and developed knowledge.

Workshop hosting will be rotated among participating organizations. Host sites will be selected for the relevancy of real situations for analysis and for the relevancy of a defined solution-need of real concern to the host. The host will provide meeting facilities and equipment, a light breakfast, lunch, liquid refreshments throughout, and appropriate people to brief the situations for analysis and solution exercises.

Forum staff will provide workshop facilitation, workshop procedures, exercise instructions, initial frameworks for analysis and solution development, and selected reading material and workshop details. Additionally, forum Staff will editorially manage the development of documentation deliverables, plan and cause greater-community awareness, and develop a greater-community involvement plan.

The structured workshop procedures and responsibilities are graphically summarized in Figure 2.

Initial Knowledge Frameworks

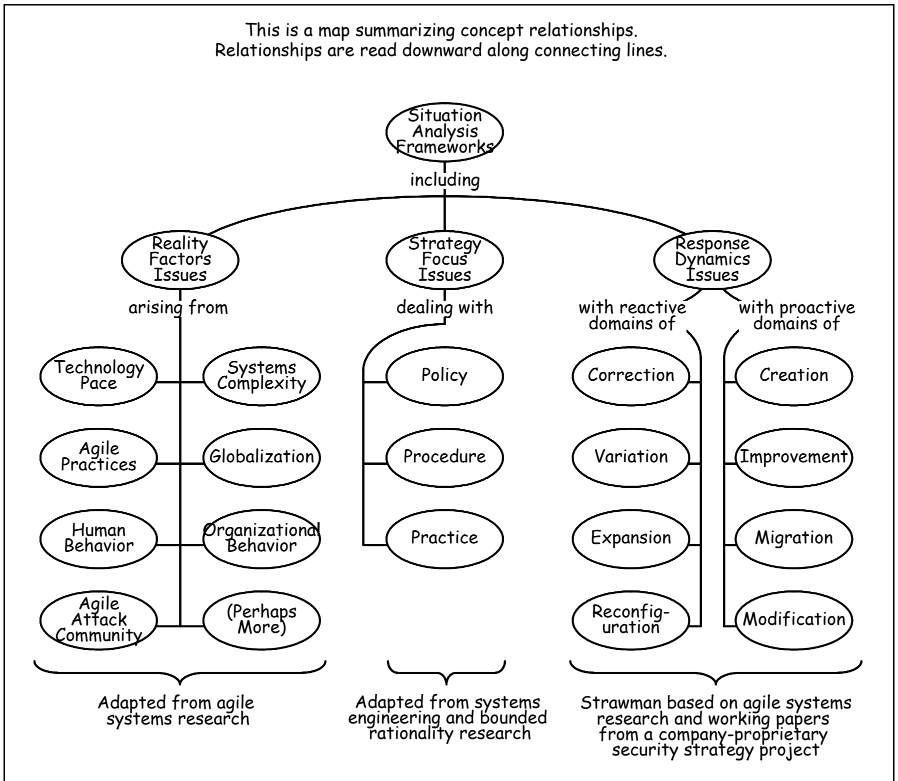
Two categories of frameworks will guide workshop activity, one for structured analysis and one for solution-fitness profiling. The frameworks outlined in this document are *initial* frameworks, and are expected to undergo adjustment in use as appropriate. Their purpose is to structure the workshop effort for productivity, effectiveness, and consistency.

There are three *analysis* frameworks: the Strategy-Focus Framework structures the elements of security strategy, the Reality Factors Framework structures the seven issue-focus areas of rational strategy, and the Response Dynamics Framework structures the proactive and reactive dynamics within the functional elements of strategy. There are also three Solution Fitness Frameworks: the Agile Response Framework structures the elements of a specific solution strategy, the Agile Design Framework guides an agile solution design architecture, and the Solution Excellence Framework defines and guides solution quality. These frameworks channel thought and activity for analysis and profiling, and are presented as preliminary starters, with the expectation that they will evolve with use.

Strategy-Focus Framework - Security strategy in the large consists of policies, procedures, and practices. In order for any of these to be effectively rational they must be aligned with the realities of the security environment, as opposed to an unsustainable wished-for set of conditions.

To be precise, these terms are defined as used here - attempting to specify comprehensive and unique intent, and eliminate ambiguity and intermixing found when comparing the actual use of these terms across organizations.

- Policies are organizationally approved objectives. They typically manifest as a controlled document, augmented often with undocumented tacit organizational and cultural understandings. They include principles governing general and contextual expectations, regulatory compliance, level of acceptable risk, human behavior, and tradeoffs between quality of service and security needs.
- Procedures are organizationally approved methods. They typically manifest as a controlled document, augmented often with undocumented tacit organizational and cultural understandings. These include controls and process methodologies.


This is a map summarizing concept relationships.
Relationships are read downward along connecting lines.

Adapted from agile systems research

Adapted from systems engineering and bounded rationality research

Strawman based on agile systems research and working papers from a company-proprietary security strategy project

Figure 3 – Pathfinder Initiative – Situation-Analysis Framework Tools

- Practices are organizationally intended executions of policies and procedures. They manifest as deployed network infrastructure, deployed appliances, deployed software, deployed services, and actual human activities.

It is recognized that approved procedures may not reflect policy accurately, and that approved practices do not necessarily achieve an accurate implementation of policy and procedure. Not because any are willfully suborned or knowledgably inadequate, but rather that they may be unknowingly insufficient, cause unanticipated consequences, or simply be the victim of human error and behavior.

It is further recognized that policy is often insufficiently defined, naive regarding the virulence of the attack community and ignorant of what is rationally sustainable under real operating conditions. Such a policy cannot guide the design of effective procedure and practice.

Policy is where reality is recognized or not, and practice is where reality bites. Alignment of policy and practice is determined by procedure. Rational practices will only occur to the extent that rational policies drive rational procedures.

This framework will guide the overall focus for analysis, ensuring that knowledge deliverables can be acted upon for immediate effect. Table 1 summarizes a breakdown of this framework.

Policy (Objectives)	Procedure (Methods)	Practice (Execution)
• Principles - general and contextual expectations, and organizational behavior. • Regulatory compliance. • Acceptable risk. • Human behavior. • Tradeoffs between risk and user productivity - employee/ management users and customer/ supplier/ collaborator users.	• Controls - code quality assurance, audit trails, practice audits, personnel monitoring and validation, enforcements, etc, • Process methodologies - Governance, disaster recovery, sys admin rules, hiring/firing rules, code quality rules, external organization interconnect, identity management, patch management, service level agreements, etc.	• Networks - internal and external connectivity infrastructure. • Appliances - hardware/ software development, acquisition and life cycle management. • Applications - software development, acquisition and life cycle management. • Services - acquisition and life cycle management. • Activities - procedure execution and management.

Table 1 - Analysis Functional-Focus Framework

Reality-Factors Framework - The reality issues were introduced in "Rectifying The Information Security Gap" [1], a paper that highlighted the fundamental underlying reality generally mismatched by current security approaches. Here they are revisited as forces we are all familiar with, but tend to ignore when developing strategy. The purpose of this framework is to guide the analysis activity to recognize and articulate how reality issues impact current policy, procedure, and practice.

1. Technology pace - Increasing pace of new product and service introduction is inevitable: globalization is broadening the supplier and innovator community, and a growing knowledge base accelerates the spawning of new ideas. For users, new security incompatibilities and problems are discovered in the proving grounds of new and unpredictable usage modes. For developers, testing naturally limited by unanticipated usage consequences and past experience with older and different technology defies perfection. The effect of pace is not unknown: At Gartner's 2004 Security Summit Victor Wheatman warned "... each new wave of technology will render existing information security measures obsolete, increasing security exposures in new and legacy environments [2]."

2. Systems complexity - Increasing complexity is inevitable as networks grow and interconnect on larger scales, and as network nodes, hardware and software alike, grow in sophistication. For users, unanticipated consequences *are* the consequence. For developers, the combinatorics grow exponentially beyond the ability of controlled design comprehension. The effect of complexity is not unknown: Edward Tenner notes in *Why Things Bite Back* that “The complexity of ... systems makes it impossible to test for all possible malfunctions and makes it inevitable that in actual use, some great flaws will appear that were hidden from designers [3].”

3. Agile practices - Increasing agility is the strategy guiding organizations in a decreasingly predictable dynamic environment, evidenced by the outsourcing rush of production and business practices, rapid growth of web services, and the rising call for transparency and everything *on demand*. For both users and developers alike, business strategies, business models and business practices are in a permanent state of flux. The imperative for enterprise agility is not a secret: the *2004 Global Security Survey* by Deloitte Touche observes that "Creating a competitive advantage out of environmental turbulence requires ... institutions to maintain strategic flexibility that enables them to better prepare for what they cannot predict [4]." Meta Group's Dale Kutnick notes: " The networked economy will emphasize business agility (for collaboration, mergers-acquisitions and divestitures) and demand new IT infrastructures to support it [5]."

4. Globalization - Buying, selling, producing, and developing has become distributed worldwide for most companies of any size. Underdeveloped countries are racing to become party to globalized economics. For users and developers this means partnering with people of different cultures with different ethics, values, norms, and practices; this means a

broadening supplier base of interconnected new technologies; and this means more sources of vulnerability, well-heeled nations in competition, and increased pressure to take business risk.

5. Human behavior - We are wired they way we are. We are the source of human error as well as pressured expediency. We make decision every day, all day long, as coders, as product releasers, as system administrators, as corporate decision makers, and as users. For users and developers this means inadequate policies, procedures, and practices, as well as policy suspensions, procedure shortcuts, and practice screw-ups. The effect of human behavior is not unknown: we all resonate to Murphy's law stemming from his original statement that " If there is any way to do it wrong, he'll find it [6]." George Spafford in a recent Earthweb article notes that "In 2003, a CompTIA study found that 63 percent of security breaches were attributable to human factors. In this year's study that number rose to 84 percent despite heightened awareness. Today's IT security model is broken and this is not a technology issue [7]."
6. Organizational behavior - Business is goal oriented to exploit new opportunity, and to do so quickly. The laws of first entry advantage and market share growth are inescapable drivers. Neither local optimality (within a company) nor global valuation (greater community) are observable characteristics of organizational decision making and behavior. For users and developers this means expedient decisions prevail. The reality is well known: Paul Simmonds, global information security director for British conglomerate ICI Plc, said it plainly at the recent Black Hat Briefings, "Everything we do -- business, security, anything -- is now business-driven. Your projects have to have a return on investment. Cost savings is the management mantra. And speed to market is quite often the enemy of good security. If you haven't noticed it yet, we've lost the war on good security [8]."
7. Agile attack community - Scourge technology has advanced to the point where zero-hour attacks refer to the time it takes from release to massive Internet presence, and zero-day the time it takes from new discovery to vulnerability exploitation. Attack methodologies and tool technologies are freely shared among a loosely coupled shadow community. Large scale grass-roots retaliation occurs when independent personal reactions weigh-in patriotically on national disputes or indignantly target companies on the wrong side of a thought-community. Amateur and professional alike benefit from this global collaboration of independent resources. For users and developers this means a growing, increasingly capable, and extremely agile adversary. The only way to survive against such an adversary has been known for a long time in systems theory as Ashby's Law of Requisite Variety: "The larger the variety of actions available to a control system, the larger the variety of perturbations it is able to compensate [9]."

The consequences of ignoring reality are not unknown. We cannot escape the drive and the need to progress. But we can do this with eyes open by recognizing the underlying causes and inevitable consequences, and mitigate them systemically with rational policies, procedures, and practices.

Response-Dynamics Framework - Understanding a problem space effectively today requires an understanding of the dynamics that constantly change its nature. A problem stated in today's immediate and static terms is a fleeting characterization, as the environment that causes and defines the problem continues to change. The agile systems work of the nineties developed a general framework for analyzing a problem in terms of its dynamics, and resulted in problem characterizations that accommodated change [10]. The purpose of this framework is to cause consideration of specific types of dynamics that reshape a problem space.

The framework structures *change* into two general categories: reactive changes that are responses to demanding external events, and proactive changes that are internally initiated with intent. A patch procedure may change, for instance, in response to an increased frequency of patch releases for an operating system. A policy change may be initiated, for instance, to support a new acquisition strategy.

Within each of the two general categories are four subcategories. There is no claim that these are absolute characterizations of all possible types of change, but they have proven effective at stimulating comprehensive thought.

Reactive change subcategories include:

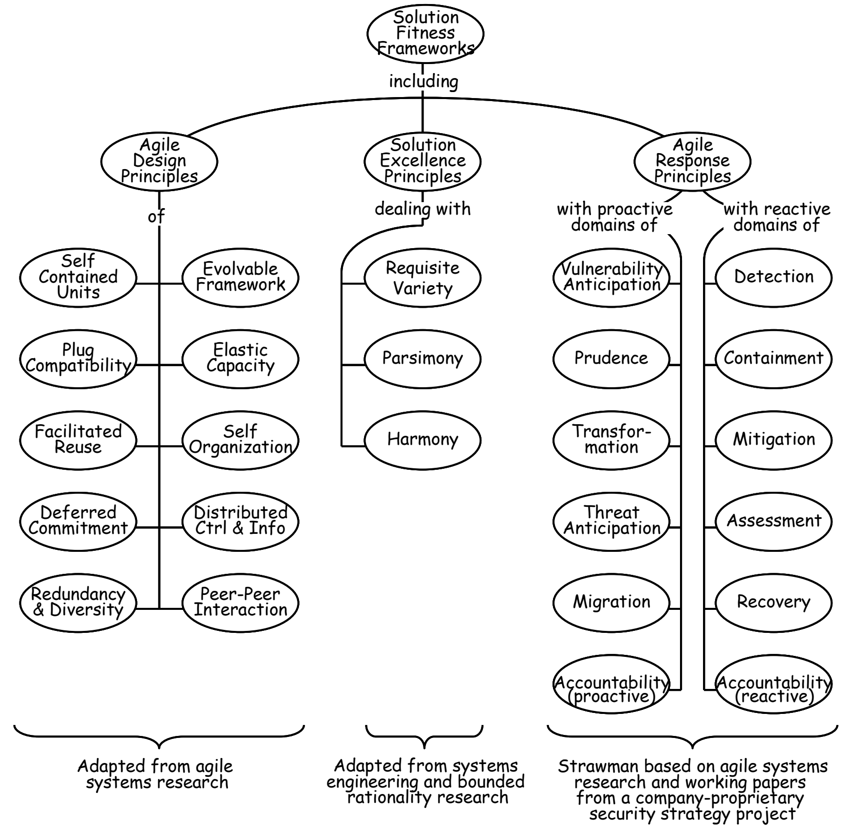
1. Correction: Rectify a dysfunction. Issues are generally involved with the failure to perform as expected, recovery from malfunction and side effects, and the rectification of a problem.
2. Variation: Real-time operating change within the mission. Issues are generally associated with operational activity, and performance and interaction variances which must be accommodated.
3. Expansion/Contraction: Increase or decrease of existing capacity. Issues are generally involved with quantity and capacity changes, when either more or less of something is demanded or desired.
4. Reconfiguration: Reorganize resource or process relationships. Issues are generally involved with the reconfiguration of existing elements and their interactions, sometimes with added elements as well.

Proactive change subcategories include:

1. Creation/Elimination: Make or eliminate something. Issues are generally involved with the development of something new where nothing was before, or the elimination of something in use.
2. Improvement: Incremental improvement. Issues are generally involved with competencies and performance factors, and are often the focus of continual, open-ended campaigns.
3. Migration: Foreseen, eventual, and fundamental change. Issues are generally associated with changes to supporting infrastructure, or transitions to next generation replacements.
4. Modification: Addition or subtraction of unique capability. Issues are generally involved with the inclusion of something unlike anything already present, or the removal of something unique.

Agile-Design Framework - That agility must be an inherent and fundamental underpinning to any effective security strategy is clear from the increasing uncertainty of the environment, growing variety of vulnerabilities, and the agility of the attack community.

This is a map summarizing concept relationships.
Relationships are read downward along connecting lines.



Solution Fitness Frameworks
including
Agile Design Principles
Solution Excellence Principles
Agile Response Principles
of
dealing with
with proactive domains of
with reactive domains of
Self Contained Units
Evolvable Framework
Plug Compatibility
Elastic Capacity
Facilitated Reuse
Self Organization
Deferred Commitment
Distributed Ctrl & Info
Redundancy & Diversity
Peer-Peer Interaction
Requisite Variety
Parsimony
Harmony
Vulnerability Anticipation
Prudence
Transfor-mation
Threat Anticipation
Migration
Accountability (proactive)
Detection
Containment
Mitigation
Assessment
Recovery
Accountability (reactive)
Adapted from agile systems research
Adapted from systems engineering and bounded rationality research
Strawman based on agile systems research and working papers from a company-proprietary security strategy project

Figure 4 – Pathfinder Initiative – Solution-Fitness Framework Tools

Once the security environment is recognized in terms of its dynamics, its solution must be agile to at least a corresponding degree. Design principles for agile systems were discovered by examining hundreds of such systems for common fundamentals [10]. Design principles apply to a system of defined modules interacting according to a standards framework, for common purpose. Ten principles emerged as generally present:

1. Self-Contained Units (Modules) - Components are distinct, separable, self-sufficient units cooperating toward a shared common purpose.
2. Plug Compatibility - Modules share defined interaction and interface standards; and are easily inserted or removed.
3. Facilitated Reuse - Modules are reusable/replicable; and responsibilities for ready re-use/replication and for management, maintenance, and upgrade of module inventory is specifically designated.
4. Evolving Standards (Framework) - Frameworks standardize inter-component communication and interaction; define component compatibility; and are monitored/updated to accommodate old, current, and new modules.
5. Redundancy and Diversity - Duplicate Modules are employed to provide capacity right-sizing options and fail-soft tolerance; and diversity among similar modules employing different methods is exploited.
6. Elastic Capacity - Module populations may be increased and decreased widely within the existing framework.
7. Flat Interaction - Modules communicate directly on a peer-to-peer relationship; and parallel rather than sequential relationships are favored.
8. Deferred Commitment - Module relationships are transient when possible; decisions and fixed bindings are postponed until immediately necessary; and relationships are scheduled and bound in real-time.
9. Distributed Control and Information - Modules are directed by objective rather than method; decisions are made at the point of maximum knowledge; information is associated locally, accessible globally, and freely disseminated.
10. Self-Organization - Component relationships are self-determined; and component interaction is self-adjusting or negotiated.

The purpose of this framework is to guide a solution fitness profile compatible with the dynamics of the issues being addressed.

Agile-Response Framework - An agile environment cannot be addressed successfully by rigid proscribed solutions. Instead, by expressing the requirements of a strategy, and each of its constituent elements, in terms of a fitness function, proposed solutions can be filtered for acceptability before specific features are weighed against alternatives. This approach recognizes that each operating environment has its own unique and changing characteristics, and guides consideration of proposed solutions with unique and innovative insights.

The framework below recognizes that a strategy based on perimeter defense is insufficient, and that security measures will be breached when the reward for success is valued or the strategy for protection ignores reality. In the end, the technical infrastructure is not the weakest link.

Reactive Principles

1. Detection – Detect intrusion and damage quickly
2. Containment – Minimize potential damage scope
3. Mitigation – Minimize potential damage magnitude
4. Assessment – Understand what has been damaged and how
5. Recovery – Repair damage quickly
6. Accountability (Reactive) – Identify the perpetrators forensically, after damage

Proactive Principles

1. Vulnerability/Risk Anticipation – Identify pending changes to vulnerability and risk before occurrence
2. Prudence – Correct vulnerabilities before exploitation, sense indirect indicators of pending exploitation
3. Transformation – Change randomly the elements/nature of security system
4. Threat Anticipation – Identify and counter threats and risks before exploitation
5. Migration – Continuous upgrade of security strategy and components
6. Accountability (Proactive) – Identify perpetrators with traps, glass houses, disinformation, etc, before damage

Solution-Excellence Framework - This framework is an initial strawman based on established systems engineering theory and research in bounded rationality [11, 12, 13, 14]. During the project this framework may undergo some augmentation with additional categories, while it is expected to undergo considerable refinement and descriptive expansion specific to security excellence within categories.

1. Requisite Variety - Provides functional quality by observing Ashby's Law: "The larger the variety of actions available to a control system, the larger the variety of perturbations it is able to compensate....variety must match variety."

2. Parsimony - Leverages Occam's Razor to arrive at the simplest effective solutions and reduce unintended consequences.

3. Harmony - Provides aesthetic quality by engendering user comprehension, trust and respect, principally by supporting rather than inhibiting human and organizational productivity and goal priorities.

Conclusion

The Pathfinder Initiative develops new knowledge on two fronts:

1) Defines problem nature - By defining the problem in terms of compatibility with natural forces, we will compel a matching solution with an irrefutable argument. The value is that we will know the requirements which a solution must address.

2) Defines solution nature - By defining the solution in terms of an agile fitness function rather than narrowly proscribed methods, we will engage a broad front of unrestricted thinking and searching. The value is that unpredictable innovative solutions will emerge.

Clear value accrues immediately to participants, who develop a first-hand appreciation and insight for the situation and its required actions. Policies, procedures, and practices will be viewed in new light, and altered accordingly.

The alternative is to continue muddling through and hoping for the best, perhaps justified by the unspoken thought that "I am managing quite well, thank you, I am still employed and making things happen. And my performance is as good or better than anyone else's. Clearly evident by the fact that I and my organization continue to survive."

This initiative will have historic consequences. It will be the first development of a strategic view of information security strategy issues, environmental reality, and effective action.

In speaking to the compelling pursuit of progress, its consequences, and its responsibilities, Scott Yoder observes: "We are 'technological creatures' -- using technology is part of the human condition. Technological power + human ambition = both great achievements and horrible disasters. Unintended consequences are inevitable. Nevertheless, we are responsible both for what we do and what we fail to do with technology [15]."

Target start date for the first Pathfinder Initiative workshop awaits commitment of a sufficient number of Pathfinder commitments. If you feel resonance, and would like to hear more about Pathfinder Initiative participation for your company or yourself, send your comments and state your interest to Rick Dove at rkdove@AgileSecurityForum.com, or visit www.AgileSecurityForum.com.

References

1 "Rectifying The Security Gap", Rick Dove, June 2004, www.AgileSecurityForum/Docs/AsfPaperConceptCall.pdf

2 "Gartner predicts less money for security spending", Shawna McAlearney, Security Wire Perspectives, 6/10/2004, www.searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci969563,00.html

3 *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*, Edward Tenner, Sagebrush Bound, 1997.

4 *2004 Global Security Survey*, Adel Melek, Deloitte Touche, May 2004, www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_SecuritySurvey2004_051704.pdf

5 "The Externalization Imperative", Dale Kutnick, CIO Magazine, 12/15/98, www.cio.com/archive/010199/view.html

6 "Murphy's Law Origin", Chris Monkman, www.murphys-laws.com/murphy/murphy-true.html

7 "Getting at the Root of Security Problems", George Spafford, Earthweb, April 27, 2004, www.itmanagement.earthweb.com/secu/article.php/3345901

8 "Beyond Borders: Losing the Perimeter to Gain Better Data Security", Anne Saita, Security Wire Perspectives, 8/2/2004, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci996078,00.html

9 *An Introduction to Cybernetics*, W. Ross Ashby, Chapman and Law, 1956, http://pespmc1.vub.ac.be/ASHBBOOK.html

10 *Response Ability: The Language, Structure, and Culture of The Agile Enterprise*, Rick Dove, Wiley, 2001, www.parshift.com /ResponseAbility/Preface.htm

11 *Administrative Behavior*, Herbert Simon, Free Press; 4th edition, 1997

12 *A Behavioral Theory of the Firm,* Richard Cyert and James March, Blackwell Publishers, 1992

13 *Choices, Values, and Frames,* Daniel Kahneman and Amos Tversky (Editors), Cambridge University Press, 2000.

14 *Value Propositioning - Perception and Misperception in Decision Making*, Rick Dove, Iceni Books, 2005

15 "Frankenstein Today", Scott Yoder, http://www.msu.edu/~marianaj/frank2.ppt

Rick Dove

Rick Dove is CEO of Paradigm Shift International and Chairman of The Agile Security Forum. He was educated as an electrical engineer at Carnegie-Mellon University, did graduate work at UC Berkeley toward a PhD in Computer Science, spent his early career as a systems software developer, and gravitated quickly to start-up, turn-around, and change management. He has run companies producing software products, manufacturing machinery and services, strategic planning and management services, and fine wine production. He has led engineering, R&D, IT, information security, sales, and marketing in a variety of companies. He co-patented the world's first electronic postage meter. He's created, organized, and led project consortia from proposal through operating phases with NIST, DARPA, and NSF funding, for clients such as Lockheed-Martin, Rockwell Rocketdyne, Collins Avionics, and Texas Instruments. He's interfaced with Navy, Air Force, DLA, and NIST program managers. He developed and led the National Center for Manufacturing Science's first R&D agenda, and designed and implemented its consortia collaborative procedures. He initiated the US involvement in the international Intelligent Manufacturing System consortia program. He orchestrated the Department of Defense support for the agile enterprise program at Lehigh University, was co-principle investigator on its seminal Agile Enterprise project, and led the subsequent Agility Forum research and industry involvement activity funded by DARPA through Navy and NSF channels. He went on to organize and lead independent collaborative projects that identified and developed design principles for agile systems in general, and explained their application to business systems in *Response Ability: The language, Structure, and Culture of the Agile Enterprise* (Wiley 2001). His new book, *Value Propositioning - Perception and Misperception in Decision Making* (Iceni Books, 2005) addresses decision-making behavioral reality. A full resume is available at www.parshift.com/Files/PsiDocs/RkdBio.pdf.