

Rectifying the Information Security Gap

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

Abstract: In 50 years of accelerating IT evolution, security policy, procedure, and practice has followed along as a patchwork reaction. The rate of new technology deployment, the growth of computer literacy, the complexity of systems, and the global stampede to electronic business and agile operations are running away from this approach. Today's organizational security strategies are misfit to the true nature of the problem. While the value of systems at risk is increasing, the relative value of security solutions is declining. This decline will continue unless the natural forces that shape the nature of the security problem are understood and addressed compatibly - by the organization at risk. This document attempts to illuminate the nature of the incompatibility, argue that the situation is critical, and propose a proven approach for correction.

Situation

Computing entered the business environment as a research and problem solving tool in the fifties. In the sixties when corporate records and intellectual property were integrated with electronic data processing and storage technologies a new form of corporate vulnerability and risk came with it. In the seventies remote access to these records ushered in a new set of risks and vulnerabilities, expanding the exposure beyond the perimeter of insider fraud, vengeance, and theft. In the eighties MRP took hold of operational decision making and ERP began putting much more at risk. In the nineties the movement to desk-top computing, Internet access, email communications, and electronic banking did it again, while simultaneously the percentage of the computer literate population crossed a critical threshold. Crossing into the new millennium we see corporate operations integrating with customers and suppliers, web services supporting business processes, electronically connected outsourcing, commerce over the wires, electronically transparent and real-time enterprises, mobile computing, wireless access, global collaboration, and the expectation for much more to come.

Identity theft, national espionage, competitive espionage, electronic terrorism, grass roots special-interest retaliation, organized crime, insider vengeance, insider crime, and sophisticated readily-available exploitation tools are the reality of the day. Increasing systems complexity and technology-leveraged human error bite just as bad. Couple these with insecure coding practices and a continuously changing technical landscape, and the situation is already beyond control.

Vulnerability and risk have been escalating faster than deployed security strategies, and the rate of escalation is increasing. It is ignorant of natural laws to think it is simply because people are insufficiently concerned, don't have adequate valuation methods, have inadequate security policies and enforcement procedures, are at the mercy of vendor economics and poorly written code, or see security as a cost rather than a benefit. The problem is intractable because its true nature is mismatched with today's solution approaches. Security policy, procedure, and practice has incrementally followed a reactionary path to an indefensible position.

Government regulation, legal responsibility and accountability, audit trail laws, shift-the-blame documentation, organized information sharing, get-tough-on-crime, and a call for secure coding practices are all too little. To say that they are also too late is to mistakenly think they are sufficiently effective. These tactical reactions ignore the natural forces that shape the problem.

Willy Sutton explained his focus on bank robbery in simple terms: That's where the money is. Whether the objective is financial gain, destruction, or ego, the magnitude of reward for exploiting vulnerability now makes information systems the preferred target, for amateur and professional alike. Swelling computer literacy at the same time is increasing the population of the exploitation-capable. The risk of a botched attempt is relatively low, as neither lethal arms nor physical presence are necessary. Anyone counting the unsuccessful attempts at penetration sees a feeding frenzy. Growing reward, growing capability, and relatively minor risk is increasing temptation and the ranks of active players. These trends are irreversible.

Under these conditions the relative value of deployable security technology is declining. The cost associated with risk and vulnerability is rising faster than the ROI of security countermeasures. Chasing that tail will continually increase the percentage of operating costs devoted to security and still fail to catch it. Here we will explore the nature of this predicament, and propose a solution.

Security is an issue for business, military, government, education, and all organization types that employ information technology. In the interest of delivering a clear and succinct message, the focus here is on the business community, and speaks directly to business managers and business decision makers, both as internal staff and as vendors. It is, nevertheless, understood that all types of organizations share the same predicament.

Goal

The goal proposed for the business community is straightforward: Foster development of a security strategy consistent with and responsive to the true nature of the problem.

Current security approaches are incompatible with at least seven immovable aspects of reality. We will look briefly at each:

1. **Technology pace** - The innovation engine feeds on itself, and is decreasing product life cycles while broadening the technology front with increased variety. The pace of new software and hardware product introductions is such today that the vulnerabilities exposed in service over time are not even fully discovered, exploited, and patched by the time they are superseded by newer products with newer vulnerabilities. New technology and even new products based on established technology cannot help but bring new vulnerabilities.
2. **Systems complexity** - The complexity of software systems alone have long passed our abilities for analytical predictability. Networked business operations overlaid with a networked global community have added new dimensions of combinatorics and complexity. We cannot predict with any assurance at all the results of a system change, and rampant change is continuous. Companies merge and race to interconnect; they upgrade, replace, and add new technology continuously; competition and opportunity drives evolving customer and supplier interfaces; and business operations are fragmenting and distributing business processes globally that chase changing economic advantages. The law of unintended consequences [1] expresses itself naturally in complex systems under change.
3. **Agile enterprise** - Keeping up with fast changing technologies, markets, competition, customer desires, and operational strategies is pushing companies into agile enterprise practices. Outsourced manufacturing, support services, and IT management is a strong and growing trend that enables costs and capacity to fluctuate in tune with revenues and opportunities, as they must. Web services and remote business process management enables faster deployment of new business strategy. Remote access and wireless technologies increase professional resource access and response. Real-time operation and transparent enterprise visibility necessary to manage at the speed of today's commerce web-enables control as well as status. Vendors are responding to the demand with new infrastructure technology, and application service providers are responding with new services. The enterprise operational and strategic processes are increasingly dependent on intranet and Internet accessible distributed resources that can be reconfigured and changed in tune with the quickening pace of market and economic necessity. The need for enterprise agility is only going to increase, and bring with it more and faster changes in interconnected resources and distributed operational services.
4. **Globalization** - China, Russia, and the rest of Asia are young but serious economic players in the progress of globalized commerce. The rest of the developing world is coming right along behind them. This brings more interconnected business, more technology deployment, more technology vendors, and more technology innovation. It also brings different ethics, different values, different perceptions of risk, early-learning-curve players, and nation-state involvement in gaining commercial footholds. For established players, globalization heats up the competitive environment and increases the pressure on business for faster response to opportunity. This means more sources of vulnerability, well-heeled nations in competition, and more pressure to take business risk.
5. **Human behavior** - We humans are wired the way we are. We make decisions every day, all day long, as coders, as product releasers, as system administrators, as policy makers, as corporate decision makers, as users, and as national intelligence agents. Our perceptions are biased by hopes and expectations, as well as the context that determines our immediate interests and values. We are the source of human error. A phrase that is self explanatory when it comes to operational mistakes. On top of all of this, we are whimsical. Rules are made to be broken and they are, in any event, made for others who are less wise than we. Murphy's law is not a joke. It is a law of probability accentuated by human behavior. All of this deals with people who are trying to do the right thing. But the perverse also exist, as do the incompetent inquisitives who can't resist fooling around. Optimal actions and decisions will never prevail anywhere.
6. **Organizational behavior** - Organizations are more than simple aggregations of people, whether they be producers of information technology, vendors of security products, or purchasers and users of both. Organizational behavior is determined by disparate internal demands, changing attention focus, and limited ability to consider all problems simultaneously. Decision makers have inherent conflicts which remain unresolved, power politics and positions that exert biased influence, and competing interests for limited resources. They are ruled by individual rather than group objectives, mitigate conflict by compromising greater values to achieve consensus, seek solutions that are acceptable rather than optimal, and vary risk seeking and risk averse behavior with economic conditions. On top of this, 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.

7. **Agile attack community** - Agility is the capability to seize unpredictable opportunity quickly, to thrive under changing conditions, and to vary resources and commitment at will. It is an apt description of the attack community. Scourge technology has advanced to the point where we now refer to zero-hour attacks for the time it takes from release to massive Internet presence. Meanwhile the increasing sophistication of attack development and tool technologies has already reduced the time between vulnerability discovery and exploitation to mere days. Infected machines and public distribution of attack tools mobilizes massive resources quickly. 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 loosely-connected global collaboration of independent resources. And now a spawning hatchery emerges: the nature of global outsourcing shifts the concentration of skilled programming from country to country as economic factors dictate, creating new skills in new areas and pushing experienced skills in old areas into the ranks of the disillusioned and under employed. These cited developments are less than three years old, and more will continue to come.

Implications

The increasing reward and opportunity for exploitation increases interest; and in the professional targeted-objective community, justifies increasing expense. Though we must succeed at basic housecleaning chores, such as systemic reduction of poor coding practices and at motivating better secure-code quality assurance, we can only expect to reduce the amateur background noise and shift the vectors of attack for the skilled. The urgent corrective measures on today's agenda are necessary, but at best they are only holding actions.

Watching the current reactive strategies plug new holes with hope is denial. This is a losing game. Waiting for vendors and academics and governments and blue ribbon committees to win this war is misplaced responsibility. It is time for the peasants to arise and save their own wheat fields, with the passion and commitment of those about to be overrun.

The goal is a security strategy that is compatible with the nature of the problem and the forces that shape it, rather than one that denies reality or wages a losing fight against it. Strategies that fight the natural forces are attempting to maintain this system in an inherently unstable state.

Action

It is time to take meaningful action in proportion to the urgency and opportunity - to know the nature of the problem, and then to craft the nature of a compatible response at multiple levels, from concept and strategy, through business organizational reality, to policy, procedure, practice and systems. This must be led by the community that is at risk, for they craft policy, procedure, and practice within the organization, and only they can create a demand for effective technology support, and then, only if they understand the nature of the problem and the nature of the solution in terms compatible with their priorities and capabilities. They must be actively supported by vendors of course, who must develop the same understandings grounded in the behavioral reality of the customer.

Proven Approach

Industry faced a not dissimilar situation a short while ago. Sometime in the eighties the business environment began changing faster than organizations were capable of responding. The problem was not one of late decision making, but rather inability to implement decisions quick enough. Sufficient evidence in the early nineties made this incompatibility irrefutable, when a seminal 1991 government-sponsored project focused attention and developed consensus on the unavoidable and growing criticality. Agility, the lack of it in enterprise, is the word that captured the nature of the incompatibility.

That 1991 project did nothing more than define the problem and develop broad consensus. Subsequently some of the participating companies along with Lehigh University sponsor-funded the creation of the Agility Forum, to develop knowledge and solution strategies with open industry participation. DARPA weighed in with significant additional funds in 1994, enabling professional staff and resources for The Agility Forum, with the objectives of defining the nature of agile enterprise and the infrastructure and technology necessary to support it. Hundreds of organizations sent over a thousand representatives to participate in periodic working groups focused on different aspects of agile enterprise. Four years of organized open working group activity with four open annual conferences reported on progress by both Forum participants and others from around the world. A special working group for agenda development employed a rotating membership from key industry, academic, and government groups. A proactive outreach program briefed and sought advice from industry associations and government interests frequently, and encouraged formation of separate European initiatives.

Today business literature abounds with reference to agile enterprise practice. Business books and learned advice of all kinds address response to rapid change in one form or another. Outsourcing is a preferred strategy for obtaining resources and capabilities as needed, and discarding them just as quickly when economic cycles or market interests change. On demand computing and web services are a major focus for software vendors. These and similar

developments would have occurred in any event, for they are necessary compatible responses to the unstoppable problem of fast change. But the Agility Forum did hasten the transformation and did focus the thinking in this nation and around the world; and in the process, did create the now-emerging market for products and services that support agile enterprise.

As a principle investigator on that original project, and lead strategist responsible for setting up and managing the subsequent agenda and formal industry involvement for The Agility Forum, I recognize what we did that worked, and what we could have done differently for more effectiveness. Further refinement of working group disciplines occurred in a subsequent independent participative project that identified design principles for agile systems, with results published by Wiley in 2001 as *Response Ability: The Language, Structure, and Culture of the Agile Enterprise* [2].

In none of that work was the growing security threat to business addressed. Yet neutralizing or precluding security problems demands the ultimate in agility. It is from this perspective of lessons learned that I suggest a strategy and the five objectives that follow:

1. **Define problem nature** - If we can define the problem in terms of compatibility with natural forces, we will expose denial with an irrefutable argument. The value is that we will know the requirements which solutions must address.
2. **Define solution nature** - If we can define solutions in terms of fitness functions rather than narrowly proscribed methods, we will engage a broad front of unrestricted thinking and searching. The value is that unpredictable innovative policies, procedures and practices will emerge.
3. **Gain broad consensus on problem** - If we can gain a broad consensus on the problem across the business community, we will create a demand for technological support. The value is that a compelling market will be defined and created.
4. **Gain broad understanding of solution** - If we can gain a broad understanding of the nature of solutions, we will focus research and development on solving the real problem and help users recognize a real solution. The value is that organizations will adopt compatible policy, procedure and practice, and vendors will supply compatible products and services that address the problem effectively.
5. **Develop migration strategy** - If we can develop a migration strategy in terms of incremental infiltration and evolution of the status quo, we will open a path compatible with business decision making. The value is that action will be taken and the evolution toward effective security will begin more quickly, stay on track, and establish and maintain momentum.

User-Led Agile Security Forum - A community of practice for knowledge development, diffusion and deployment.

Ultimately a critical mass of the community at risk must come to feel both the nature of the problem and the nature of the solution, viscerally; for then, and only then, will organizational strategy change and market demand emerge. This requires knowledge development and diffusion within the community, which can be efficiently accomplished if facilitated effectively.

Knowledge development means learning. This requires active participation and resource commitment, from a community that naturally applies scarce resources to internal priorities and favors short term returns. An effective facilitation of this knowledge development, that can entice a critical mass to participate, must therefore address the need for short term returns and provide value to existing priorities. The disciplined collaborative knowledge development approach which evolved from the agile enterprise work is one method capable of accomplishing this. This method is a form of action learning and *Appreciative Inquiry* [3] known as *Realsearch* [4], for its use of real people addressing real problems in real time, learning from what works well, rather than focusing on undirected gap closure .

Importantly, real-people addressing real problems means that participants take home immediately actionable knowledge. Not knowledge and wishes that have to wait for new technology development, but rather knowledge that can drive rationality into policy, procedure and practice immediately.

A critical mass of involvement will not materialize all at once. Some companies are more ready to begin this knowledge development and deployment than others. They have priorities that can benefit now from an early understanding of the problem. If in no other ways, the significant expenditures they are currently budgeting for security can be better informed and directed immediately, and the policies, procedures and practices they are formulating and enforcing can be more effective and less costly in side effects. These are the companies that will kick start the process as Pathfinders. Their principle focus initially will be to flesh out the nature of the problem and the nature of the solution-fitness-function, generating a cogent and compelling roadmap for immediate action by Pathfinders, as well as a call-to-action for subsequent involvement by the greater community. As few as ten such Pathfinder companies is sufficient, if they range across a variety of business sectors and are committed. More could be usefully engaged. In any event, this Pathfinder Group would be augmented with invited members of the security press and research firms that can assist in communicating the call-to-action.

Expansion and a shift of focus to solution definitions can come quickly if initial results are communicated broadly, and if they clarify the opportunity and rewards with an active outreach effort that takes the value proposition to the community at large. Rapid expansion can be accommodated efficiently if the facilitation operating strategy is *chaordic* [5] - an emergent-growth operating model much like Visa in its early Dee-Hock-driven days, that leverages the participating community rather than needing linear expansion in core enabling functions.

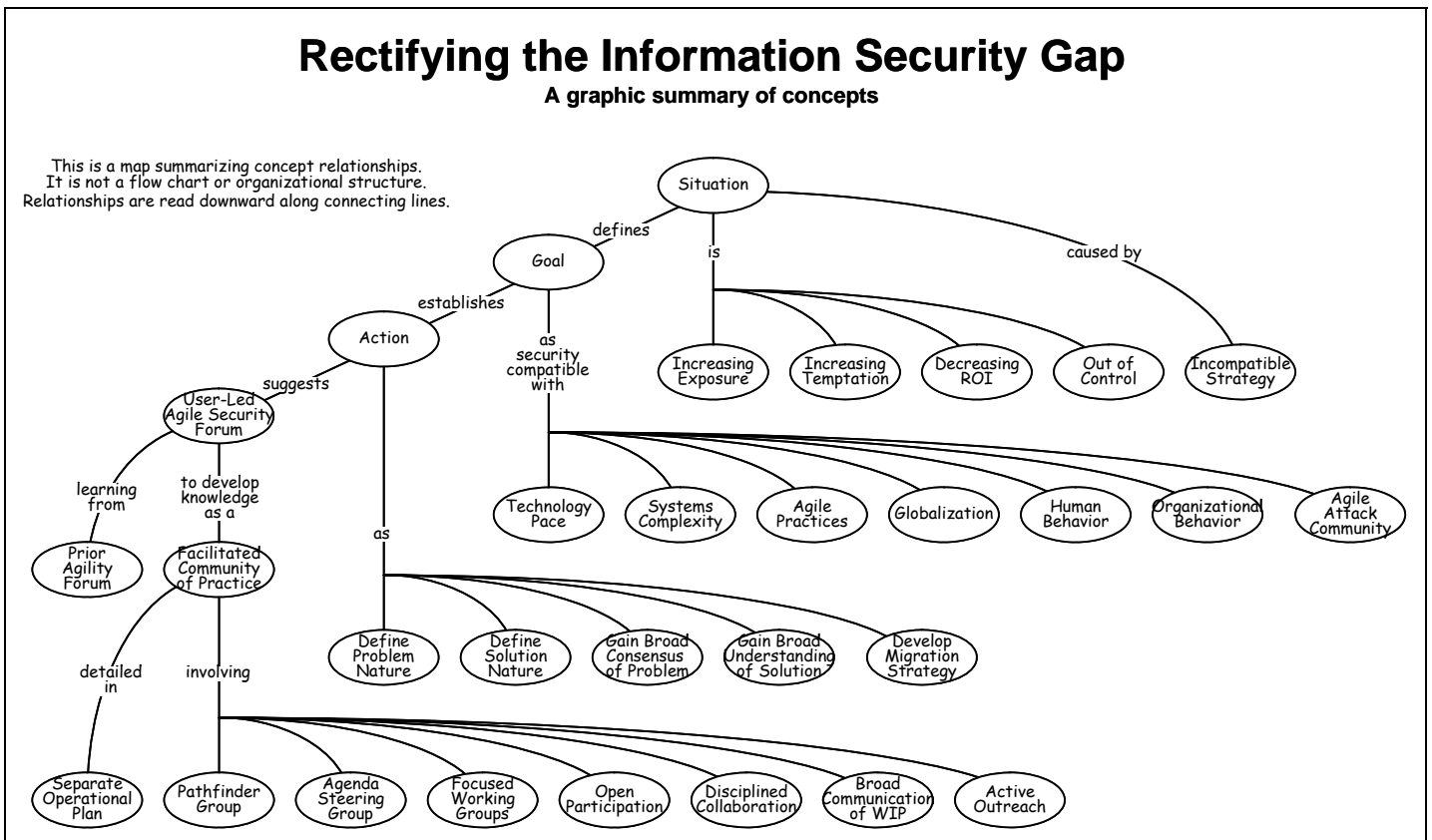
Like the Agility Forum of the nineties, knowledge would be developed by collaborative working groups established around specific focus areas, open at all times to all who are interested. These individual focus areas are limited only by the immediate interests of participants, and the ability to attract an effective chair and enough collaborators. Workshop hosting would be rotated among participant's organizations for hands-on exposure to real problems as well as real opportunities. Objective-driven collaborative groups have been shown to be effective in two-to-three day sessions that occur six-to-nine times over a 12 month period. New knowledge has to be developed, assimilated, and matured, so time plays an important role. Logistics, procedures, and communications are supplied by a core facilitation staff, so that participants can focus exclusively on objectives and solutions.

The effectiveness of cross-industry working groups is often problematic. Disciplined collaborative workshop procedures, similar to the Reasearch approach mentioned earlier, have proven to be highly productive. An appropriate version of these disciplines would be employed to insure that value is incrementally delivered for participation. Two important elements of these disciplines include frameworks for both problem analysis and solution fitness. These common frameworks facilitate both knowledge convergence and transfer, and should profitably leverage the related frameworks developed for agile systems analysis and design.

There is value in having a special working group that focuses on identifying the elements of an overall agenda. This agenda steering group would be populated by rotating invited membership. Their function would not be directive, but rather proactive and instigative, in that they would identify areas in need of focus, assist in finding appropriate chairs, and instigate sufficient interest to form targeted focus groups.

Companies send participants to working groups because their involvement promises immediate value. These participants are the people responsible for understanding and solving problems that have corporate priority. Participation offers leverage through collaboration with others who have similar interests and urgencies but different perspectives. Companies will not view this as an investment in professional personnel development, but rather as an opportunity to have others help them understand and address their problems effectively and immediately.

Real problems addressed by real people in real time - with actionable results. This is the underlying formula that



attracts participation. Productivity is what sustains participation. Its formula is based on a structured workshop discipline, facilitated cross-group synergy, staff support to the working groups, and an agenda steering group.

In Preparation

The incompatibilities outlined above encompass technology practice as well as policy, procedure and human practice. The finger pointing between the using community and technology providers has legitimacy for both parties, but only to a limited extent. Human behavior and organizational behavior are dominant roots of bad coding practices and poor quality assurance, as they are of poor policy and poor policy enforcement. They, like the other natural forces outlined above, must be recognized for the ever present rule they exert in the greater system composed of technology, humans, organizations and commerce. Current cries for more respect and attention to coding and policy must succeed, but they must do so in concert with the forces at work, or they will have little real effect beyond assigning blame unequivocally.

Problems are not fully recognized until some inkling of a solution separates them from just living with the way things are. The outline above of the problem and a method for addressing it is intended to generate that inkling.

It is premature to propose solutions in any detail until thoughtful agreement exists about the nature of the problem among a sufficient ready-to-act group. A quick read of what has preceded is unlikely to accomplish that.

If you feel resonance, and would like to know more about Pathfinder Group participation, send your comments and state your interest to Inquirey@AgileSecurityForum.com, visit www.AgileSecurityForum.com, and/or download the Concept of Operations document [6].

Additional Reference:

[1] Unintended consequences - www.econlib.org/library/Enc/UnintendedConsequences.html

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

[3] "Appreciative Inquiry: A View of a Glass Half Full", J. Lewis and D. Van Tiem, *Performance Improvement*, International Society for Performance Improvement, September 2004, www.ispi.org.

[4] Realsearch - www.parshift.com/docs/rsrch00.htm

[5] Chaordic - www.parshift.com/Speakers/Speak009.htm

[6] Agile Security Forum Pathfinder Initiative - Concept of Operations, www.AgileSecurityForum/Docs/AsfPaperConOps.pdf

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 formation 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. He is author of *Response Ability: The language, Structure, and Culture of the Agile Enterprise* (Wiley 2001) and *Value Propositioning - Perception and Misperception in Decision Making* (Iceni Books, 2005).