

Systemic Security Management:

**A new conceptual framework for understanding
the issues, inviting dialogue and debate, and
identifying future research needs**

Laree Kiely, Ph.D. and Terry Benzel



SYSTEMIC SECURITY MANAGEMENT

Laree Kiely, Ph.D. and Terry Benzel

“It is exponentially more difficult to build something from scratch than to destroy something that has been built. For that reason, we must build into our systems the mechanisms to protect and preserve what has been created, mechanisms that are equal to the effort we put into creating things.”

INTRODUCTION

Scope and Purpose

This paper was commissioned by the Institute for Critical Information Infrastructure Protection (ICIIP). Its purpose is to create a working document aimed at opening and promoting the rigor of dialogue and debate about nation-wide security issues. Beginning with the micro level, we will look at security issues from the standpoint of organizations themselves. Our discussion applies to all types of organizations, corporate, publicly owned, privately owned, non-profit, educational and governmental and we go beyond the focus on information to a broader definition of security issues.

Background

In February 2003, the White House released the *National Strategy to Secure Cyber Space*. That document responded to an urgent need for users, operators, and vendors of networked data and communications systems from both public and private sectors to work together to improve the security of the nation’s information infrastructure. The *National Strategy*, consistent with published policies of U.S. Homeland Security, proposed a roadmap for the future that included: 1) prevent cyber attacks against America’s critical information infrastructures, 2) reduce national vulnerability to cyber attacks, and 3) minimize damage and recovery time from cyber attacks that may actually occur.

Those goals lead to a list of critical priorities which include: 1) a national cyber security response system, 2) a cyber security threat and vulnerability reduction program, 3) a cyber security and awareness training program, 4) a secure government cyber space, and 5) international cyber security cooperation. For more detail, see <http://www.whitehouse.gov/pcipb/>.

The Institute for Critical Information Infrastructure Protection (ICIIP)

ICIIP is both a “Center of Excellence” and an “Organized Research Unit” at the Marshall School of Business, University of Southern California. It was formed as a direct response to the challenges of the *National Strategy to Secure Cyber Space*. ICIIP’s mission is to close the gap between the current state of U.S. corporate information security risk and the achievement of what is needed to protect our nation’s critical information infrastructure, again, as reflected in the *National Strategy*.

More specifically, ICIIP’s strategy is to create a partnership between business and government to narrow the security gap and, at the same time, adding to the mix as many academic resources of insight and objectivity as possible. Accordingly, and in support of the intended partnership, ICIIP has taken on five core activities: 1) awareness, 2) executive education and training, 3) research, 4) developing standards and best practices, and 5) technology assessment.

ICIIP’s Conceptual Framework: A Different Point-of-View

Historically, security in organizations has been studied and thought of in terms of the timeworn, two-dimensional components of people, process, and technology. These elements continue to occupy our concern, and we will of course make recommendations as to improved security policies and procedures that affect these historically defined elements. However, the conceptual framework of ICIIP goes significantly beyond this traditional model.

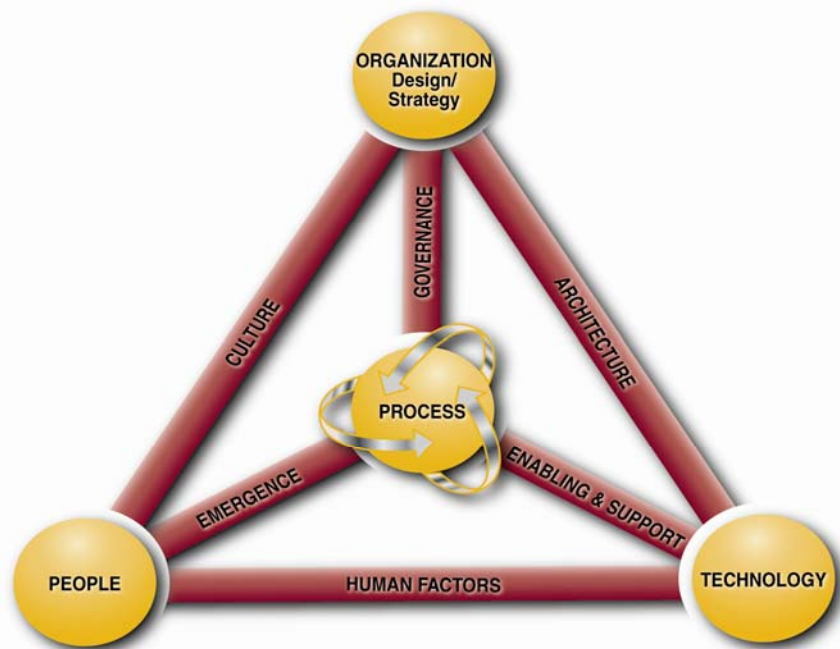
We shall argue here that the real array of problems we face and their intended solutions lie well beyond the historic perspective; that simply hardening the traditional three elements or “nodes” by more clearly defining, doing more research, and attempting more rigor in the three areas, is not enough. We shall see that, in order to become fully secure organizations, we must include focus on a fourth node-- that of organization strategy and **structural design**. The traditional triangle now becomes a *pyramid*, three-dimensional, dynamic, and also complex.

Another change: we contend that significant work must be done to understand the connections and interactions among these (now) four multi-dimensional elements. These connective relationships or interactions we will identify as *tensions*, specific relationships or connections among the nodes requiring our attention and study.

The added elements of the fourth node and the six additional tensions will probably be seen to make security issues more complicated; you might say that’s the bad news. But the good news is that they may also point us to where the more nuanced and effective solutions lie. Accordingly we shall propose that organizational systems, incorporating multiple disciplines, must be designed and put in place in order to align and manage all those complex interactions. Therefore, this white paper devotes a significant amount of attention to the understanding these of dynamic tensions, as well as to the solutions to security needs they will both illuminate and also require.

The ICIIP Model

The following diagram represents the typical organizational entity, key elements of its security system, and, perhaps for the first time in the discussion of national security issues, the dynamic relationships or “tensions” among these elements. The diagram identifies the three traditional elements of *people*, *process*, and *technology* and then adds a fourth “node” of *organizational strategy and design* to create a three-dimensional working model, best visualized as a pyramid. The connections between the nodes are shown as six dynamic interconnections, which we refer to as “tensions,” a term chosen to underscore the dynamic and often competing and conflicting roles each plays among the others. These tensions are: *governance*, *culture*, *architecture*, *enabling and support*, *emergence*, and *human factors*. In order to advance our security issues, all of these interactions--these tensions--need to be further assessed, better measured, and much better understood.



To sum up the ICIIP Model and its rationale, we intend to show that security issues have been studied too simplistically, as a somewhat static and two-dimensional collection of three independent issues. To do it justice, security needs to study not only a three-dimensional concept (with the added issue of organizational design), but also requires an appreciation and understanding of how people, process, technology, and organizational design all interact among themselves to create that complex mix of elements and issues that the question of security really is.

To begin the discussion of this model, please consider a preliminary explanation of each of the “nodes” and their interactions or “tensions”.

Nodes

Organization, the (newly added) first node, focuses on the need to design organizational structures and strategies that enable the enterprise to compete effectively, create competitive advantages, understand its tolerance to risk and adopt governance policies that elevate security to a first priority, a board level issue, pervasive throughout the enterprise. Attention to it should also take into account the multiple tensions of culture, architecture, and governance, through which it plays out in the organization.

Process, the second node, means the explicit, formal means by which things get done in an organization. This node requires enterprises to decide and adhere to those policies that administrators and users should enact to keep their organizations secure. These policies and processes should involve all levels within an organization, up to the executive C-suite. Again, though, process security is complicated by the multiple tasks and tensions of governance, emergence, enabling & support that connect it to the whole.

Technology, the third node, is specifically assigned to develop and implement technological approaches to the protection of information systems, approaches that must stay ahead of the competing, threatening technology that would exploit and corrupt those systems if it could. This will require “hardening” the node, but also improving the tensions of the “architecture” of the organization, dealing with human factors like collaboration between vendors and users, and attention to the technology role in enabling and support, to achieve optimal security.

People, the fourth node, represents the human resources in an enterprise who need to practice not only fundamental security “hygiene,” but also (and especially in more complex enterprise systems), receive added training for securing enterprise data and communications, etc. It is perhaps obvious, that the human factor is vital in the managing and perfecting of security, but this model adds concerns for culture and emergence as added tensions that must figure prominently in any enhancement of security.

To further understand and think about the above model, please realize that the three-dimensional pyramid you see here should not be reduced to two-dimensions, even though it appears here on a two-dimensional page. As much as possible try to visualize a three-dimensional pyramid, and what is even more difficult, please try to imagine a three-dimensional *discussion* as well. In a systemic, three-dimensional, and dynamic model, all aspects interact with one another simultaneously and complicatedly, just as Systems Theory posits. If you change one part of the system, all parts are changed. Further, the most flexible part of the system has the most effect and control over the system as a whole. In such a system, and especially when it comes to security, we ought to achieve perfect balance, however impossible. It’s impossible, because of the forces of entropy and dynamism that are always at work, but we strive for it. To use a metaphor from a

linear model, it's like spinning plates...just as you get one plate to spin nicely; the others you spun earlier are slowing down and in danger of crashing.

So as you read the following and try to think about this problem three-dimensionally, please imagine that you are “double-clicking” into all the branches and arteries and by-ways, all interconnected and overlapping, more like a molecule than a chain, and then, if you would be so kind, forgive us for attempting to make sense out of three dimensions while operating in two. It is, itself, a “tension.” Also, although our pyramid is meant to be comprehensive, we do not intend to repeat all of the research or science or literature on each of these nodes and tensions (as a side note, if you look in the back of many OD books, you will not find the word “security” in most indexes). Our focus is on security itself, and the viability of the model overall rests on theory and research we believe our readers will find to be familiar, merging many different fields, including OD, HR, management, IT, risk management, crisis management, security, asset protection. This paper intends to merge these ideas with an overlay of security, to show these fields’ effects on security and security’s effect on these fields.

At the end of this paper, we include a list of references on specific topics and fields of expertise. For example, for crisis management see Ian Mitroff and Larry Barton. For work on organizational design read Jay Galbraith, and for high performance issues, refer to Ed Lawler et al at the Center for Effective Organizations. The authors here (Kiely and Benzel) also invite you to read any of our other publications.

Systemic Security Management (SSM)

ICIIP believes that to be effective in protecting their information infrastructure, enterprises need to take a *Systemic Security Management (SSM)* approach to security. The SSM approach aims to ensure that an enterprise does not just buy security, but genuinely *buys in*. Similarly to Total Quality Management and Customer Service models, the result will be not only heightened security, but also the realization that buy-in creates “security that pays for itself” (See the SSM continuum enclosed as an attachment to this document).

We will also suggest that SSM is an approach appropriate not only for individual enterprises, but also for collective alliances nation-wide and, in some cases, globally as well. Systemic Security Management (SSM) is a management approach to security which serves the extended enterprise, going well beyond the boundaries of the company to include not just people, process, technology and organization, but also partners, suppliers, customers, and communities. As upper level management and corporate boards have become more actively involved in overseeing the security systems of their organizations, a set of enterprise-wide values, ethics and cultural norms has emerged that carries over to other organizations and their leaders. SSM is built around a set of core principles whose intent is to ensure an optimal balance of protection, while maintaining the ability to share information and develop innovations among strategic partners. It is an approach designed to make it possible to do business in a highly integrated way, yet ensuring that digital assets, intellectual property and proprietary technologies are protected. (*ICIIP* and Steve Rayner, *American Center for Strategic Transformation*)

Thus, with an overall purpose to help establish the extended, nation-wide SSM protocols, we begin the discussion inductively at the single organizational level, then work outward to the industries, the US, and then issue a call to global action.

Additional Goals for This Discussion

It has been said that technology has the shelf life of a banana. Shorter still, perhaps, is the shelf life of a white-paper treatise on security and technology. By the time this paper gets distributed, much of what is written here will be refined, changed, or perhaps even made obsolete by the shifting sands of rapid change in organizations and society. But we press on, because this is paper is not meant to be the last word. Our greatest hope is that it might be the *first* word, the opening shot in a rigorous dialogue and debate as well as the beginning of changes that are critical to our survival. A second purpose for this paper is to define and explain a new framework by which to view organizations and their complexity. One use of this framework, we hope, will be to better understand how to make organizations safer and more secure. A third purpose for this paper is to create a series of questions and a format for further research. So here is our invitation: Read, question, think, critique, react, disagree, add. Help us, in an open dialogue, to develop new models, new ways of looking at the issues of safety and security, new research, new theory. Ironically, although the paper is about the protection of property, we hope that these thoughts will become open property and owned and remodeled by all.

Defining “Security”

Although information and data security initially prompted this discussion and this paper, we will define the concept much wider, for two important reasons. First breaches of security in an organization are rarely purely defined and limited to one aspect of the enterprise, such as data storage or stolen intellectual property. Any breach or problem has effects that extend throughout the entire system, as we have argued above. It follows that security issues overlap and are involved in many of the crises that threaten organizations, and therefore it makes sense to consider the security of the organization as a broadly defined set of threats, catastrophes, and crises, for all of which we need protection.

Secondly and happily, as we look ahead to some of the security solutions to be proposed later in this paper, these solutions will address much more than just information security. They will also offer protection against the very array of widely defined crises that represent the real line-up of threats to the general security of an organization, an industry, and the nation as well. So we will include not only data security, but (at times) all assets, both tangible (life, limb, property, data, money) and intangibles (goodwill, credibility, reputation, knowledge, relationships, social capital, knowledge capital).

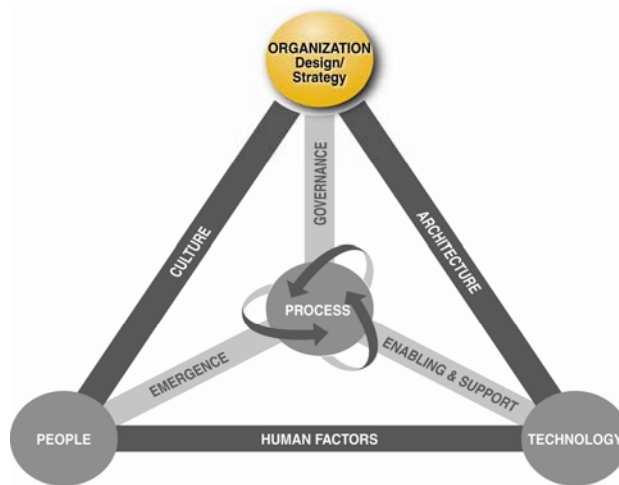
We will discuss a security problem as a real or potential compromise of safety/security and/or damage to tangible or intangible assets. These problems or breaches may be Systemic (caused by the system, or organizational design or culture), internal (coming from internal personnel) and/or external (coming from competitors, customers, press, terrorists, natural disasters, etc.). Further, they may be intentional (brought on by persons

intending harm), unintentional (brought on by persons not realizing the harm, while trying to accomplish something else), and those that fall in-between or in combinations of the above.

Again, security breaches and other crises, to the extent that they overlap, sometimes come from the same cause, and often can be prevented by the same, systemic, protective measures, should not be separated out arbitrarily from a discussion of security. We opt here for the inclusive, the systemic, the overlapping, the interrelated, the complex version of security, in order to find solutions that work, real solutions that will themselves necessarily be inclusive, systemic, overlapping, interrelated, and complex.

The Nodes...

ORGANIZATION



We begin the discussion of this first “node” in our pyramid with the observation that organizational design (or “structure”) will require careful consideration because of the subtleties of the effect of structure on all other aspects of the organization. And of course, for our purposes here, we are particularly interested in the effects of structure and design on security.

The Formal Organization

Organizational design is one of the oldest areas of systematic study of organizations, traditionally focused on the structure of the organization. For example, the traditional organizational flow chart came about as a result of Frederick Taylor’s asking questions about the organization of business at the beginning of the industrial age. Because the field was new, the only places Taylor could look to for comparison were churches, farms and the military. Churches were not the place to look because business can claim no direct divine component, and since farms were mostly family-based, so they were not an apt comparison. So Taylor benchmarked the military (of course, he didn’t call it benchmarking), and many of his observations and recommendations for business came directly from the command/control approach of the military.

Today, we have found much of that original work to be obsolete. The organizational chart is a good example: its original purpose was to depict the flow of information, the coordination of effort, and the command structure. Accordingly, the lines that connected the boxes were really arrows pointing (flowing) downwards, showing who was responsible *to* whom. Today, the question of flow of information and responsibility is, itself, a different question: we ask instead, who is responsible *for* whom? But as you may know, many organizations keep the old version in play; they see themselves along the old, antiquated, militaristic design. Ironically, many of these old assumptions have been abandoned by the military itself.

The Informal Organization

We now know that work doesn't really get done through the formal boxes on the org chart, and neither does security. If you were to map the flow of influence in your organization (a "sociogram"), you would find that real influence flows through multiple "hubs" that have very little relationship to the formal org chart. A hub is often a person with high levels of influence and information in the system. These persons are shown to have multiple linkages that connect them widely throughout the organization. Their many connections often exist because of *informal* power, credibility, influence, and expertise, qualities that the old-style organizational charts never see and therefore never portray.

So which of these is real? Mostly the *informal*, because when you come right down to it, an organization, at its core, is a network of people and information interacting with each other. That is the genuine, functioning organization that gets the work done, and our precise point is, *that* is the organization we must secure and protect. Henry Ford was reputed to have said, "I don't need people to bring their minds to work, I just need their hands and feet." Today, we often do not even need the hands and feet (as many off-site employees never "show up for work"), but we need their minds and their information and their network, and we need it to be secure. It gives new urgency to the old but newly invigorated rule that the way an organization is designed determines both what it is able to do, and also what the problems are going to be.

Among old vestiges of the past that die slowly, we can remember when our appreciation of the informal design of an organization was as something peripheral, and that the organization's formal design warranted our greatest vigilance. But consider more recent research that has shown the opposite:

In our studies on productivity, we have found four causes of lower output. First, and contrary to what managers usually think, we are finding that lower productivity is most often caused by a system flaw. These flaws (there are twelve possible) vary from poorly designed reward systems to poorly designed floor plans to systems that are so bent on compatibility that they have not had an original idea or taken a risk in years. The cause is something intentionally, but naively, designed into the organization. If people aren't doing the job, it's most often because they are diligently and faithfully following a badly designed system (Kiely, 2004, p 6).

As a segue into strategy considerations, the reader may have noticed that we combine elements of both "strategy" and "design" into the single node of "structure"; this represents a collapsing of two areas often treated separately in Organizational Design literature. Here, the collapse is intentional, aimed at emphasizing how closely strategy and design must be, if we are to advance the cause of security. We repeat for emphasis: for purposes of security, design and strategy in a well-functioning organization are so closely interrelated, we can and should treat them as two aspects of one vital element of the organization and its preservation. The "structure" of an organization that needs protection and preservation consists of both strategy and design.

Strategy

One good definition of strategy is:

“...The company’s formula for winning. The company’s strategy specifies the goal and objectives to be achieved as well as the values and missions to be pursued; it sets out the basic direction of the company. The strategy specifically delineates the products or services to be provided, the markets to be served. And the value to be offered to the customer. It also specifies sources of competitive advantage and strives to provide superior value.” (Galbraith, 2001, p. 10).

Because we extend our security concerns to include other than profit making organizations, we would adapt this definition to the more generic: “An organization’s formula for successfully accomplishing its *raison d’être* or purpose.” But we would also add that every organization must now add to its purpose statement, a *preservation* statement. This should make any organization more viable to its stakeholders, whether they are shareholders, volunteers, customers, community members, personnel, or others. Thus our overarching recommendation: it is no longer enough to communicate to the world of stakeholders why we exist and what constitutes success, *we must also communicate how we are going to protect our existence.* (Kiely, Libertas Press, 2006).

That general rule suggests some specific recommendations of steps to be taken:

- Develop a strategy for preservation alongside a strategy for progress.
- Create a clearly articulated purpose and preservation statement.
- Inform and educate all persons who work in the organization as to this dual purpose
- In strategic planning of the organization, each individual and unit must demonstrate alignment with both the purpose and preservation standards.

Note: Although these steps in the strategy may be insufficient to fully change the norms of an organization, at least the change starts here, with these recommendations.

Design

It is easy when delving into the depths of Organizational Design to stay down for long periods and come up for air only occasionally. It is a fascinating and complicated subject, beyond any detailed summary we might attempt here. But for our purposes around security, we note that Galbraith, in his justifiably famous treatment of the subject of organizational structure, makes two things stand out sharply. First, he makes the point that structure “...determines the placement of power and authority in the organization” (Galbraith, 2001, p. 11), and second, he does not mention security as part of this authority or its attendant structure. This curiosity would be typical of many current texts and theoretical books on organizational design or structure.

We think this is dangerous, and requires a shift in our thinking about the structure (design and strategy of an organization). If security concerns are urgent, then it follows that the greatest urgency is here: organizations should be designed in such a way as to protect the structure and the strategy system-wide. An obvious, but arguably urgent example, would be where in the organizational structure do we place the oversight of security? Such a pervasive system-wide issue would seem to warrant oversight and coordination at the highest levels.

But typically, oversight of security is often diffused among many “boxes” deeper in the organization chart: safety of physical assets may be in one “box,” risk management in another, maybe IT in a third, and financial assets watched by audit committees in yet another box. And typically, many of these areas report to different executives. As we have already shown, however, security is a concern, not just of different departments or different types of assets; it is a concern of the organizational whole. Security arenas overlap closely and systemically, and a breach of one affects all. We have a situation today where very often no one is responsible for the big picture. Today, at least in larger organizations, security must be housed in the c-suite: Consider perhaps a CPO or CSO.

One interesting (and somewhat scary) sidelight: organizations sometimes talk about security issues as “crisis management.” The definition of crisis is “a major, unpredictable event that has potentially negative results. The event and its aftermath may significantly damage an organization and its employees, products, services, financial condition, and reputation” (Barton, 1993, p. 2). The very term “crisis management” seems to imply a sort of ah-oh-stuff-happens-and-we-better-respond-to-it-effectively attitude. But, as we have seen in the last few years, it can take only a matter of hours, not years to destroy an entire organization; a mere handful of people, internally or externally can do the job; new assets are vulnerable because of inability to foresee all of their weaknesses and vulnerabilities; and rapid change keeps everybody off balance. We can’t wait until it happens to reactively jump into action.

So please consider: *it’s time to take the word “crisis” out of crisis management.* Crises and threats to security are not anomalies or add-ons or little bumps in the road, they are big and bad and potentially lethal, embedded in what we do, daily, hourly, *inherently*. And security management is simply *management*; it belongs inside, built directly into the structure of an organization, spliced like a gene directly into its DNA. Experts like Ian Mitroff have been making this case for years; now it is the hour for the issue to pass from the experts into expertise, from idea to practice, from “crisis management” to comprehensive, systemic security.

Call to action:

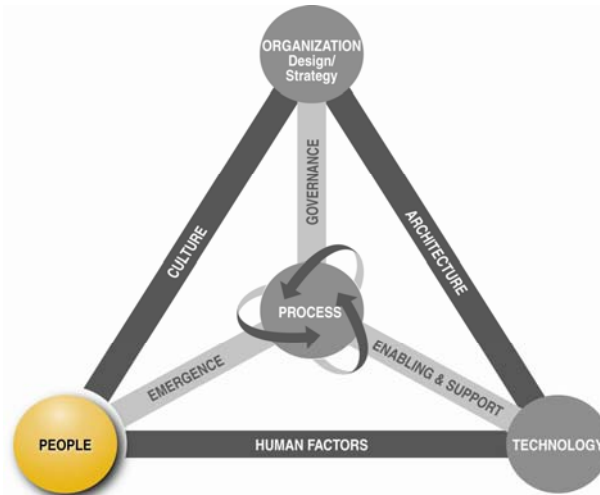
We invite dialogue and debate here

Case Studies:

Additional readings

The Nodes, cont'd...

PEOPLE



Compromises to safety and security, whether intentional or unintentional, almost always involve people either as cause or effect or sometimes both. For that reason, we consider the “People” node in the diagram early on. Borrowing from Jay Galbraith’s definition of the “people” factor, we note that the “people” node of our pyramid:

...governs the human resource policies of recruiting, selection, rotation, training and development. Human resource policies—in appropriate combinations—produce the talent required by the strategy and structure of the organization, generating the skills and mind-sets necessary to implement its chosen direction. ...Human resource policies also build the organizational capabilities to execute the strategic direction (2001, p 13).

This node is in some ways the most basic and the least controllable because it is the “baggage” that people walk in with. The first security ‘portal’ or entry point into an organizational system resides in its hiring practices. Most companies are still very lax in this area. Unless the job is considered “high security”, questions regarding security are rarely on the list of interview questions or reference checks. In fact, most organizations still do not do reference or background checks. We argue here that, although some jobs represent more potential risk to security than others, all jobs are now “high security.” The first place to find data on security issues is a person’s own private background information, which is now readily available through many on-line companies.

Defining the “People” Node

In our model, this node represents human resources and the security issues that surround them. To begin, notice that security concerns are affected by sheer numbers of people.

The larger the organization, the more diverse, and the more international or global, the more likely are breaches to safety and security. This judgment includes not only salaried employees, but also contracted or hourly people, and these may be on-site or virtual. In fact, we include all people whose efforts must be coordinated in order to accomplish the goals of the organization. And just to recognize how very complex this element of organization security really is, we must also keep in mind that “people” are not just units of one, each individual comes with all the baggage of the multiple dimensions of individuals: raw talent, skills, personalities, motivations, biases, diversity, ability to produce, values, behavior styles, choices, backgrounds, loyalties, and hopes and dreams.

Consider the case of Maria who unintentionally sent an email stream to her vendor. This vendor, as is often the case, also served some of Maria’s company’s competitors. Deep in the email stream was a piece of critical, confidential information that would give away a stealth competitive strategy. “I was in a hurry and the vendor needed the information right away. It never occurred to me to erase the rest of the email stream. They’ll never go back and read all of the previous emails. Besides, we can trust this vendor.”

To enhance security within the “people” node, it is critical to see these people issues systemically. As such, it will be necessary to make revisions to most existing HR policies and processes, revisions that are security-related. It may not be necessary to design a whole new, comprehensive model for HR, but instead, we need to look for areas where we can suggest a significant add-on to existing HR policy. Our recommendations include the following:

1. Job Descriptions

All job descriptions must include a “level of security risk” and some content containing the handling of information. Examples might include:

- Creating a risk-rating system for each job category in all organizations
- HR and management/supervisors rewriting job descriptions with security in mind
 - Defining security
 - Creating levels in all definitions
 - Below is a “Rating System” example:

1=low 10=Extremely high	Job type	Cashier	Data manager
Type of risk			
• Data security		1	8
• Fiscal security		5	1

2. Recruiting and Selection

Security can be enhanced at the level of recruiting and selecting candidates through the following.

Recruiting:

- (1) First consider where you are conducting your recruiting activities:
 - (a) Sources
 - (b) Executive search
 - (c) Universities
 - (d) Competitors

- (2) Second, use above type of rating system with these recruiting sources to apply to persons they recruit and hold them accountable for implementing this model. Demand that they must demonstrate policies that fit your criteria. This helps create self-regulating systems so that new laws and government regulation may be unnecessary.

- (3) Third, consider the following regarding candidates:
 - (a) Find out how much information the recruits have about your company
 - (b) Find out who recommended the candidates
 - (c) Use “Hypothetical Situation” interviewing skills
 - (d) Interview for ethics and judgment
 - (e) Gather data on previous experience thinking in terms of security behaviors

Selection:

Consider adding to your existing HR policies:

- (a) Doing background checks that go beyond previous employers and criminal records
- (b) Having HR and candidates future manager work together to select and hire
- (c) Create a clear employment contract that includes security expectations
- (d) Make very clear upon hiring what IP belongs to the employee and what belongs to the organization

Selection Case Study Example

A small manufacturing company in the US (before 9/11) was hiring a contract negotiator who would interface with the US government (DOD) as a client. The man was brought in to interview because he was a friend of one of the current employees. There was an urgent need for this position to be filled because the company had been having trouble meeting the DOD’s requirements and they were in danger of losing the contract. The fellow looked great on paper, his friend vouched for him,



they felt lucky to have found someone so qualified so quickly. It was a slam-dunk. So they hired him on to get him rolling and asked HR to do the due diligence simultaneously to his first few weeks. HR reluctantly agreed. When the personnel officer asked the man for his references and his college transcripts, he said he would get back to them but he was really busy getting his job done and moving forward with the client. HR asked several times for his information, so finally, in an act of apparent frustration, he handed them his transcripts. HR promptly reminded him that the transcripts had to come directly from the university to be considered legitimate. HR then received a copy of the man's transcripts that had been notarized. The personnel officer's suspicions increased, so she called the state and county where the notary was and found out there was no notary by that name anywhere in the state. HR then called the university from where the transcripts arrived and found out that no person by that name had ever matriculated at that university.

Note there are multiple dangers here. Not the least of which is that this fellow had committed fraud (felony?) and his name might be on some of the contracts with customers as a representative of the company. The organization decided their vulnerability was too much so they decided not to file charges, but to simply have him escorted out of the building.

He soon found another job, and no one called for references. In the case of the felon negotiator, the danger was minimal because the man had lied in order to get a job, not for industrial espionage. But that is a slippery slope. Testing for moral character is difficult, but doing a background check isn't.

Civil Liberties

A strong word of caution is necessary here on the importance of the "people" node and *civil liberties*. People, even in the paranoid 21st century, still have the right to privacy and it must be honored. Organizations also have rights, including contacting references, academic institutions, and, on occasion, previous employers, etc. One question that should be asked during these allowable reference checks is: how did the person treat confidential information?

- a) Draw the line between what is acceptable in seeking a person's background and what is an offence of civil liberties. Make this public and very clear inside and outside the organization.
- b) Create a new and rigorous hiring system that focuses on security as one of the qualifiers, while keeping in mind an individual's civil liberties.
- c) Train managers and team interviewers in interviewing skills, especially hypothetical situation interviewing techniques
- d) Develop a strong focus and train HR personnel in the issues of screening for security consciousness.

- e) We want to screen for potentially damaging personnel before they get into the system and manage people inside the system to maintain optimal safety and security attitudes and behaviors. This follows the old adage “Hire hard so you can manage easy.”

Placement and Rotation:

When placing new employees, rotating or promoting current employees:

1. Use committees in larger organizations for making these decisions
2. Employ recruitment and selection criteria (listed above) for internal rotations as well.

Skills, training, and development (in security behaviors and attitudes):

When training or developing employees in security behaviors:

1. Begin during employee orientation. Conduct separate training sessions on security issues so new employees won't get overwhelmed with early data and forget what they learned.
2. Conduct a second training for employees after they have been in their position for 6 months
3. Conduct regular update sessions over time for current employees
4. Measure the learning effect of training
5. Avoid simply putting the information on the security behaviors and concerns in a policy and procedures book

Rewards systems and HR policies:

When implementing reward systems, reinforcement measures, and overall personnel policies, it is necessary to focus on the following to ensure better security behaviors:

1. Consistency: critical here for balance in the eco-system. If inconsistent, the policies and behaviors create cultural tension due to lack of alignment between the organizational design and the people in the system.
2. Formal reward systems (define policies regulating salaries, promotions, bonuses, profit sharing, stock options, and so forth): adjust to provide motivation and incentive for the alignment to the strategic direction.
3. Informal reward systems (The subtle ways people are rewarded: appreciation, attention, reinforcement, better assignments, etc.): sometimes these rewards have more effect on the people than the formal rewards. Paying attention to the ways people are reinforced can create a “strong situation” and mold the culture to be the way we want it to be. Failure to do this may create a culture that brings out the very behaviors we are trying to avoid. We largely get what we reinforce.
4. Clarity: People respond positively and as a group to situations where all persons see the issues clearly, *and the same*. Later we will develop the concept of a “strong situation” (see the culture section), one element of which is this “clarity” issue.

Performance feedback:

None of the above recommendations are sustainable if management fails to conduct appropriate effective and disciplined performance feedback performance reviews.

For these to be effective, we recommend:

- 1) Determine if there is a deficiency and decide if it is attitudinal or skill based
- 2) If it is skill based, then ensure the training includes:
 - a) Safety and security attitudes and behaviors of managers
 - b) Review more than once a year, and supervisors must ask security-type questions. For example: What information are you worried about holding that you think might be proprietary. And, how safe do you feel and why?
- 3) Performance reviews must have a rating section regarding protecting the enterprise and organizational health. (For more details see Microsoft's new performance review program)

Physical placement of human resources (on-site, flex-office, virtual, etc.):

This is a fairly new issue and very security-related, as organizations are encouraging more flexibility in the work environments and/or are reducing the expenditures on property and space. In information security alone, we have to ask about home computers, how many users, are they left on all night, etc.? Some organizations are trying to invent a way that software can flag critical info while it is being passed from person to person. Although this topic overlaps with architecture and technology, we have placed it here because it is also a profoundly human issue. (For further information on a model for developing, training and testing virtual environments, see Kiely's Chapter on International Virtual Executive Teams in *Advances in Global Leadership* (2001). For state of the art information on workplace configurations and alternatives, contact Sun Microsystem's Open Work Practice Group or go to www.sun.com/openwork)

Cautions/Recommendations:

- High performing organizations demand decentralized decision-making and people must be allowed to speak to one another. Without the free flow of information, organizations will be paralyzed. Caution, "better security" can become "Unable to produce."
- Nationally, self-regulating systems are preferable over new laws.
- All employees and stakeholders must be system "ecologists" protecting and preserving the enterprise whether we actually "go" to work or not.
- We must be careful not to destroy the very liberties we are seeking to protect

Conclusion: The building of trust and loyalty starts with the formal people policies, but certainly doesn't end there. As you will see, the way an organization is designed can be the cause or the solution of the problem. Later, we will argue that the fundamental solutions and problems may lay in the tension between Organization and People: that of organization culture.

Call to action:

We invite dialogue and debate here

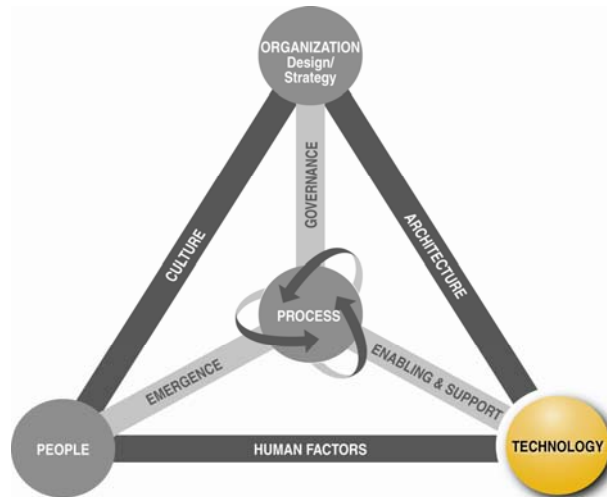


Case Studies:

Additional Readings

The Nodes, cont'd...

TECHNOLOGY



Technology is one of the traditional and still vital nodes of the ICIIP model. It is integral to the protection of information systems. It is the arena of the continuing “arms-race” with cyber criminals and terrorists, so any account of security must include technology at the leading edge of the fight. Thus, technology must be pervasive and constantly evolving, providing layered security, security for collaboration and business processes, and architectural organization security.

Information security technology is one of the fastest growing segments today and it is available in many forms and flavors. The earliest information security technologies were virus tools to protect desktop computers and firewalls to protect organization boundaries. Technology and the threats it is designed to counter have expanded ten-fold. Today one can find security technology to protect individual users, enterprises, intra-nets, internets, home users, small businesses and every combination and flavor in-between.

Available Types of Information Security Technology

In general, information security technology falls into several broad categories:

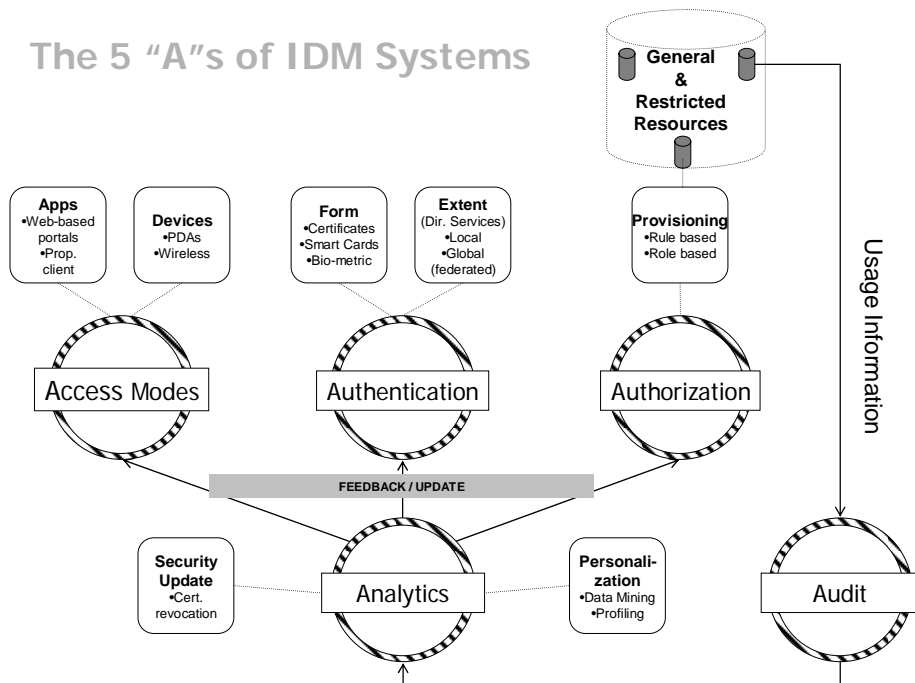
- Security Design and Configuration
- I&A: Identification and Authorization
- Enclave internal
- Enclave boundary
- Physical and environmental

Technology for *security design and configuration* has largely grown out of the field of Change Management and generally consists of configuration control tools and process tracking technology. The focus here is on cataloging, auditing and managing an organization’s systems. This area has received increased focus as a result of the Sarbanes-Oxley which is discussed further under Governance.

Identification and Authorization technology is a very important and often misunderstood area. Not only does an enterprise need to identify and authorize people and processes,

but there needs to be a clear connection between such I&A technology and access control *policy* that is embedded in and part of the policies of overall security of the organization.

I&A technologies include simple passwords, single sign-on systems, challenge response systems, and public key infrastructures. The task is to choose a technology that allows and organization to a) reliably and consistently identify users, b) verify that the identity presented belongs to the person that it is assigned to and c) connect a valid identity to an authorization for a specific set of accesses. Therefore Access, Authentication and Authorization, while separate issues, must work hand-in-hand. They must also be linked to a system that permits Analysis of the resulting activities and a way to Audit the system's performance. This "Five A" Identity Management Model, developed by El Sawy, Chellappa, and Griffith for SIM is portrayed in Figure 3 below from the final report.



Technologies for an organization's *internal or enclave* protections generally fall into the category of desktop protection and have traditionally been the province of anti-virus technology. In recent years, however, many of these technologies have moved from the desktop to a client-server enterprise solution. Desktop or server-based internal enclave protection technology is oriented towards detecting known bad behavior with predictable patterns. Other internal enclave technologies include I&A discussed above and auditing, configuration management, and accounting. The general threat of the "insider problem," which refers to an authenticated and authorized user actually mis-using his or her access, is still a very complicated problem, with very few technological solutions available. Lacking specific technology, the "insider threat" must be countered through process, culture, and organizational behavior as discussed elsewhere in this paper under the other nodes and tensions of the ICIP model.

Enclave boundary technology is focused on protecting an organization from external forces and thus creates a boundary or border protection. The most common boundary protection technology is in the Internet Firewall. Firewalls first developed in the 90's (Ranum, 1992) are based on the philosophy of "keep the bad guys of the wild internet out of an organization's systems." There are many different types of firewalls with corresponding levels of security and manageability available today. In fact, most internet connections, routers and even home cable/dsl technology are shipped with default firewall protection. More sophisticated boundary protection often requires a higher degree of management and configuration but can buy increased protection if properly configured and maintained.

Recently the boundary protection market has expanded to include Intrusion Prevention or Detection (IPS or IDS) technology. This class of technology includes some degree of automated ability to identify an intrusion, analyze its potential impact, and then communicate specific directives to the boundary device, firewall, or network switches and routers to mitigate the risk of the attack propagating. Such technology holds great promise but suffers from two significant technological challenges. First, it is imperative to make sure that the IPS device itself does not become an unwitting victim of an attack. That is, the perfect attack is to fool the IPS device into telling all of the boundary devices to configure themselves exactly as the hacker needs to implement his attack. Second, the intrusion detection component of an IPS solution must have a very low false positive rate in order to ensure accuracy and to ensure that an organization's infrastructure is not unnecessarily closed off or shut down.

Finally, one must not overlook *physical and environmental* protection technology. Managing most information security technologies requires a high security environment and the highest level of privilege. Thus, process, governance, and culture play an important role. There are many technologies for physical and environmental controls, and as part of a well architected security process they will contribute to an increased security posture. These include physical access control devices (badge readers), biometric devices, sensors, and alarms.

Current Practice

Current practice in security technology deployment runs the gamut from the good over to the bad and the ugly. All too often one encounters technology everywhere, resulting in an over reliance on technology or using technology as a band-aid. What is needed instead is a comprehensive Security policy and "Architecture" (see "tension" section on "architecture"). Technology cannot stand alone, but when well architected and integrated into process, people, and organizations it proves to be vital and integral, providing a dramatically improved security posture for an organization. Other sections of this paper will discuss the role of technology as it integrates into all other nodes and tension points.

Recommendations

Information security technology needs to play a balanced role in a systemic security system. Security technology for protecting the interests of an enterprise must be designed as part of an overall set of systems and processes that are usable by humans and fit the organizational culture and governance. Technology should ensure that the intellectual property and proprietary technologies of individual companies are protected and secured while creating a collaborative working environment.

Edward P Yakabovicz, Information Security Officer for Bank One's Consumer Internet Group discusses recent trends in technology and the challenges of layered security technology:

Information security should be based on a layering effect of technologies throughout an organization to provide an umbrella that mitigates risk and thereby reduces threat. The introduction of intrusion-prevention systems (IPS) offers one more layer.

For the last 20 years, security technologies have been segregated to the different worlds of intrusion-detection systems (IDS), firewalls, routers, switches and more. Each operates in a separate segment of the company network, while together providing threat mitigation and risk reduction through the collection of logs, rules, policy and configurations. Although very successful, each technology requires the manpower of at least one human to manage or confirm updates. Several technologies attempt these automatic updates with, for example, firewall rules or blocking methods. With more failure than success, many are either unacceptable or unmanageable. In the end, each fails due to the amount of intelligence and manual work necessary to ensure each change does not impact the network, customers or user base. Technology does not contain the necessary Artificial Intelligence (AI) to combine the results from these systems and make the proper judgment for configuration changes, blocking rules or overall device re-configuration. There has simply not been a viable solution that works for each demand or requirements that would bind all necessary networking components together (Yakabovicz, 2003).

Call to action:

We invite discussion here

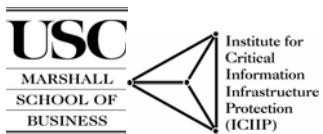
Case Studies:

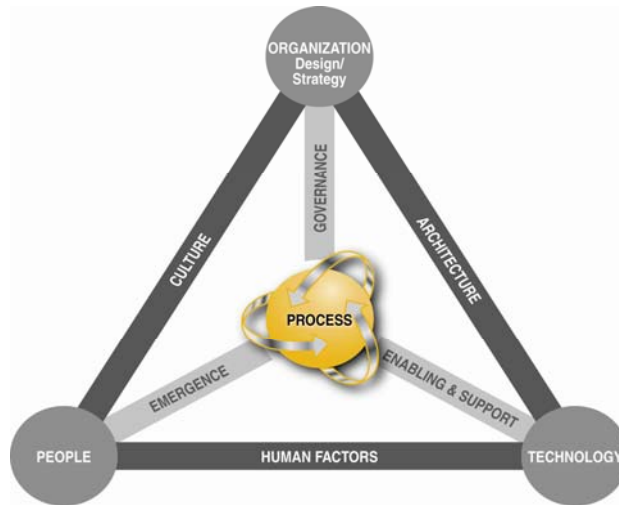
Additional readings

- NIST - Practices and Implementation - <http://csrc.nist.gov/pcig/cig.html>
- http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci936192,00.html

The Nodes, cont'd...

PROCESS





Process is a key node with vital linkages to all of the other nodes and tensions. Process cannot exist without the people to implement it, organizations to breathe life into it and the technology that is at the heart of it. The process node embodies all of the requirements for an enterprise to develop, promulgate, educate, and enforce security practices and procedures. These practices and procedures should encompass standards for all levels of an organization from the executive C-suite to users at all levels (business office functions, core functions, IT/MIS and network administrators).

The focus of this node is procedural and it can be independent of technological sophistication of an organization and in fact, encompasses many standard business processes such as risk assessment and business continuity planning. That is, it is just as important to have clear security policies and procedures around protection of a file cabinet of information as it is to protect a complex IT infrastructure.

Defining Security Process

The **Federal Financial Institutions Examination Council's (FFIEC)** web site defines Security Process as:

Security process is the method an organization uses to implement and achieve its security objectives. The process is designed to identify, measure, manage and control the risks to system and data availability, integrity, and confidentiality, and ensure accountability for system actions. The process includes five areas that serve as the framework....

- ◆ *Information Security Risk Assessment—A process to identify threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes.*
- ◆ *Information Security Strategy—A plan to mitigate risk that integrates technology, policies, procedures and training. The plan should be reviewed and approved by the board of directors.*
- ◆ *Security Controls Implementation—The acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the*

deployment of risk-appropriate controls, and assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties.

- ◆ *Security Testing—The use of various methodologies to gain assurance that risks are appropriately assessed and mitigated. These testing methodologies should verify that significant controls are effective and performing as intended.*
- ◆ *Monitoring and Updating—The process of continuously gathering and analyzing information regarding new threats and vulnerabilities, actual attacks on the institution or others combined with the effectiveness of the existing security controls. This information is used to update the risk assessment, strategy, and controls. Monitoring and updating makes the process continuous instead of a one-time event.*

Security risk variables include threats, vulnerabilities, attack techniques, the expected frequency of attacks, financial institution operations and technology, and the financial institution's defensive posture. All of these variables change constantly. Therefore, an institution's management of the risks requires an ongoing process (FFIEC web site, 2002).

Current Practice

Security process efforts are probably the most prolific area of investment over the past ten years. As organizations woke up to the information security problem, they scrambled to define security processes. Best practices, standards, policies, procedures, manuals, guidance, consulting, implementation, and corporate governance documents abound. As a result, a massive array of resources is available to organizations in the area of security process. Naturally, this has had both a positive and negative effect; it is good that organizations have invested in this important area, but all too often security process ends up being a check box on a company process form plus many boxes of documents left on shelves and unused.

Security Process concepts are at the heart of the National Strategy to Secure Cyber Space. The five recommendations: 1) a national cyber security response system, 2) a cyber security threat and vulnerability reduction program, 3) a cyber security and awareness training program, 4) a secure government cyber space, and 5) international cyber security cooperation, all require extensive use of process to define, manage and monitor cyber security programs and systems <http://www.whitehouse.gov/pcipb/>

Recommendations

Some of the most effective approaches to security process have come from the establishment of "Best Practices". Further, security process is not a binary all-or-nothing state for an organization. Thus, the approach of establishing best practices which can both be tailored to a particular organization's state while simultaneously setting an objective goal to strive for seem to have been the most successful. Best Practice activities also have the benefit of being living processes and can avoid the pitfall of documents sitting on a

shelf. An effective security process must span all aspects of Systemic Security touching on all nodes and contributing to all tension points.

The ICIP Systemic Security framework

(<http://www.marshall.usc.edu/ctm/ICIP/Graphics/Security%20Matrix%20ICIP%205%20Levels.pdf>) describes Security Process at Level 4 (Commitment) and Level 5 (Systemic) as:

Level 4 Commitment Focus

Security processes and procedures are designed to be as unobtrusive to workflow and process as is reasonable. When the nature of the security requirement is disruptive, a clear explanation as to its purpose and the need for employees to follow the procedure is communicated.

Level 5 Systemic

The primary focus is on prevention of potentially catastrophic security incidents through advanced technology, proactive planning, open communication, and workforce commitment. Many security breaches occur through “social engineering”—an intruder gains access to the network or a physical location by deceiving an unsuspecting employee. The potential of these types of crimes is minimized through regular communication between security personnel, managers, and employees. Managers regularly engage in scenario planning so as to act in a well thought through and practiced manner in the event of a security incident (pp.).

The key factors that enable security processes to be effective in these organizations are planning, communication, and measurement. Systemic organizations need to establish fully integrated policies where “process” is part of their culture, as well as the tensions of architecture, enablement, emergence, and human factors. Its role in these tensions is to be found under discussion elsewhere in this paper.

Resources

There are many good resources available to organizations looking to establish security processes. Standards organizations, government organizations and industry all provide guidance on developing security processes and best practices which can be tailored by industry, organization size, technology, human factors and many more considerations.

Among some of these are:

- IETF: <http://www.ietf.org/>
- US CERT: <http://www.us-cert.gov/>
- ITAA: <http://www.itaa.org/>

Among commercial offerings is IBM's "Security Process Assessment". This service identifies strengths and weakness in an organization's security process and consists of a review of an organization's IT processes and documentation, an analysis of the information and a report describing business approaches for process changes to improve the organization's security process.

Call to action:

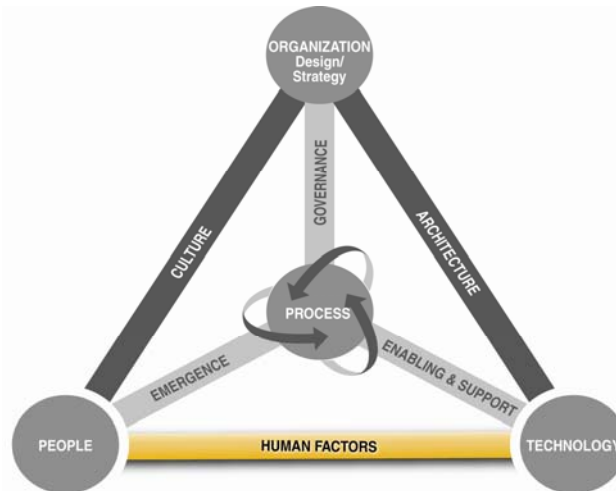
We invite dialogue and debate here

Case Studies:

Additional readings

- FFEIC IT Handbook InfoBase

HUMAN FACTORS



The tension at the base of our ICIIP Model pyramid is the area of “human factors.” This tension connects and supports the people and technology nodes. By now the reader is familiar with our repetition of the perhaps obvious, but vital point: technology alone cannot address the information security problem. But this tension makes the special emphasis that, even if all steps are taken to systemically integrate technology with the organization, architecture, culture, and processes, it will still not do the job if it is not *usable* technology.

The field of human factors and man-machine interface has received considerable attention since the beginning of information technology, yet human factors continue to take a back seat to all of the other design criteria. Lack of attention to human factors is even more an issue in the arena of information security technology. Most security technology grew out of the “hacker” (when hacking had a good connotation) community and out of that came a certain arrogance, “if you aren’t smart enough to understand it then you don’t deserve it” kind of attitude. Thus, many security technologies are designed with little consideration to the human factors or man-machine interface for usage. For example, routers designed to provide WiFi internet connectivity in homes have such a complicated encryption enablement process that most home owners revert to the default setting out of sheer frustration, leaving most such networks available for use by their neighbors or worse.

Nature and Scope of the Tension

Studies have shown that a large number of enterprise security breaches come from mis-configuration of essential security technologies, e.g., firewalls, web servers. Often the most stringent security technology requires a high degree of sophistication to install,

configure and maintain. Even the simplest routine maintenance operation can change the security protection of an organization.

Security technology must be developed and deployed with people in mind, for as we have emphasized elsewhere in this paper, it is *people* who are the final line in the protection and defense of an organization. “Tension” is an excellent word here: so called “simplified” interfaces and the tendency to automate technology can, ironically, lead to *more* insecurity because operators/users don’t know what is going on inside the box. On the other hand, overexposure of security technology to human users can lead to complexity that is beyond many technology users. These issues are the subject of ongoing debate in the security community; while there are no clear answers to the question of human factors or how people relate to technology; this is an important tension in defining an organization’s systemic security position.

In the report, “Human Issues in Secure Cross-Enterprise Collaborative Knowledge-Sharing” Dr. Majchrzak (2004, p.7-10) has identified a number of issues relative to knowledge sharing that are relevant here to both the human factors tension point and to the people and technology nodes.

First, Dr. Majchrzak identifies four areas of information security concern

1. Sharing the corporate jewels
2. Granting unauthorized Access
3. Not Following Security Procedures
4. Physical intrusion

All of these can be seen as related to the overall ergonomic question of security technology and its relationship to the people who must use it. The question that must be asked as part of a holistic security practice is: “Does the technology facilitate better security practices or does it make it more difficult for the people in an organization to act secure?”

Dr. Majchrzak reports:

To avoid these concerns of security breaches, the traditional approach is to create policies that give employees the responsibility for avoiding a breach and to provide some security technology (e.g., firewalls) to make breaches more difficult. The policies inform employees of the actions expected of them when sharing knowledge with others (or when doing any work at all). The employee is given the responsibility to change passwords often, to not give others access to a database without informing systems administrators, to not share corporate secrets, to turn off a computer when not in use, to shred documents, to regularly remove the cookies from the hard drive, to take notice of others’ suspicious behaviors, and to be given strict instructions about which documents and knowledge can and cannot be shared with others. This traditional approach has been found to not work (Schlarman, 2001). Employees still pursue their own

agendas, often with wanton disregard of security measures: they find these measures to get in the way, create additional burden for them in their jobs, and otherwise make the task of collaboratively sharing their knowledge with others that much harder (Majchrzak, 2004, p11
<http://www.marshall.usc.edu/ctm/ICIIP/Documents/Ann%20Majchrzak%20Human%20Issues%20in%20Secure%20Cross%20Enterprise%20Collaboartive%20Kn owledg%20Sharing%20White%20Paperat%20USC%20%20041504.pdf>)

Current Practice

The Computing Technology Industry Association (CompTIA) in its annual “Study on IT Security and the Workforce” May 17, 2005,
http://www.comptia.org/about/pressroom/get_pr.aspx?prid=611
reports that organizations blame 80 percent of all security incidents on human error, or on human error in conjunction with a technical malfunction.

The tension between people and technology is still heavily dominated by technology. In fact, as the rapid rise of technology continues we see technology for technology’s sake and the people are left behind. Very few organizations can get past this barrier, as the technology is simply not designed for optimal human interaction.

Recommendations

A Systemic security organization must take steps to close the gap between technology and people so that they can co-exist and create a synergistic environment.

One approach to making non-user-friendly technology more user-friendly is to provide additional training, documentation, and in some cases user-friendly interface custom applications.

Brian McCarthy, CompTIA's chief operating officer, recommends: To be truly effective in preventing and combating security threats, organizations need to take further steps by spreading security awareness and knowledge from a select group of IT staff to larger portions of their staff. (McCarthy, 2005,
http://www.comptia.org/about/pressroom/get_pr.aspx?prid=611)

On the side of social science, Dr. Majchrzak recommends:

- Include social resources in psychological contracts between employees and firm
- Encourage sharing about security risks
- Integrate security technologies and policies into the work process
- Tools must be “self-deploying” and “seductive”
- Develop policies that align individual, group & organizational concerns

- Provide tools to help employees dynamically weigh costs and benefits of acting securely
- Match a firm's information security strategy with the market

(Ann Majchrzak, 2004, p.37-47

<http://www.marshall.usc.edu/ctm/ICIIP/Documents/Ann%20Majchrzak%20Human%20Issues%20in%20Secure%20Cross%20Enterprise%20Collaboartive%20Knowledg%20Sharing%20White%20Paperat%20USC%20%20041504.pdf>)

Call to action:

We invite dialogue and debate here

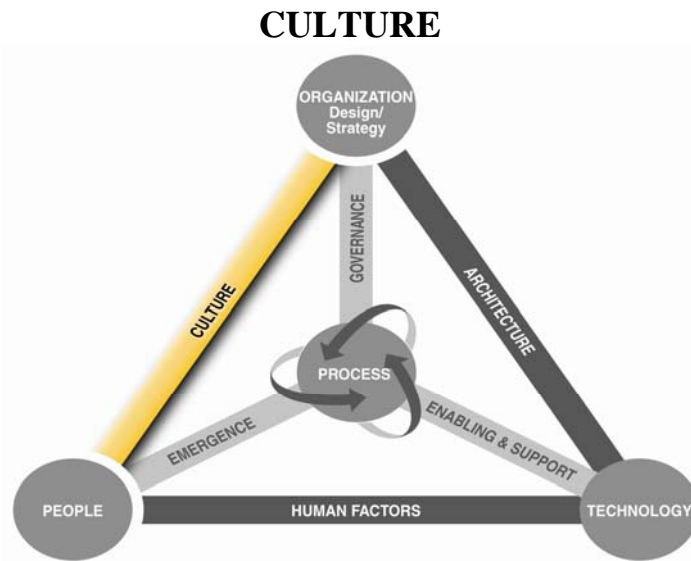
Case Studies:

See Ann Majchrzak, 2004, p.33

<http://www.marshall.usc.edu/ctm/ICIIP/Documents/Ann%20Majchrzak%20Human%20Issues%20in%20Secure%20Cross%20Enterprise%20Collaboartive%20Knowledg%20Sharing%20White%20Paperat%20USC%20%20041504.pdf>

Additional readings

The tensions, cont'd...



Over time, when we combine the interaction between the strategy and structure (Organization) and the raw human resources (People) of any enterprise, we end up with an organizational “culture.” When the two are perfectly aligned (ranging between seldom and never), we can imagine perfection. But in fact, the best we can do is constantly strive to improve the alignment of people and organization. There are ways to intervene and attempt to ensure that the culture is optimal, but for the most part cultures form themselves, often taking the path of least resistance. And they are powerful, insidious, and definitional in the life of an organization.

In previous sections, we argued for the importance of seeing security as an issue of design and strategy, needing big-picture vigilance and coordination at the highest levels of an organization. Here we make the argument that as important as structure and strategy are in matters of security, they pale when compared to the influence of organizational culture. Make no mistake about it; it is the culture, that which lies deep in the DNA of an organization, that determines its workings, its vulnerabilities, and its preservation. Thus we intend to spend some time assessing this issue of culture, in order to understand both the problems and also the opportunities for security it presents.

An organization’s culture can often have something that is already in place that creates a barrier to effective security. At the end of this section, when we propose some solutions, we will suggest the option of building an “Intentional Culture,” a set of expectations and desires throughout the organization that enlists the power of a created culture to make the organization *more* secure.

Culture Defined

As a general definition, the essence of culture is *patterns*, patterns of behavior, belief, assumptions, attitudes, and ways of doing things. More specifically, culture has to do

with the covert, *underlying* patterns of an organization. An organization's culture can, to some extent, be created through the predictability and rigor of its structure, but it often comes about due to unintended consequences of the structure or perhaps lack of structure. Usually, it's both ways: intentional and unintentional. Research shows that the synergy between people and structure make culture much stronger than just the additive effect of these elements. It is nothing less than the "how stuff gets done" of organizations. (Kiely, 2001). In addition, "A culture is not simply a collection of human and physical resources but the pattern by which these are joined, balanced, and synthesized." (Hampden-Turner, 1990, p. 12-13).

Culture is emergent, it is learned, and it often creates a sense of superiority and comfort. It is also passed to succeeding populations who tend to make the same assumptions of superiority, predictability, and comfort.

In our own research on international teams we found:

Chronologically, we could put it this way: cultures evolve as a type of shared history because a group of people goes through a set of common experiences. Those similar experiences cause certain responses. The responses become a set of expected and shared behaviors. Those behaviors become unwritten rules, which become norms that are shared by all people who have that common history or are descendants of that original group.

By the time these commonalities become rules and norms, they have become pre-conscious, or even unconscious; they are a part of us. They become reality—truth, beauty, and justice, and we believe our norms to be the "right" ones and others to be weird, incomprehensible, rude or just wrong." (Kiely, 2001).

...culture reflects assumptions about clients, employees, mission, products, activities, and assumptions that have worked well in the past and which get translated into norms of behavior, expectations about what is legitimate, desirable ways of thinking and acting. [These] are the locus of its capacity for evolution and change. (Hampden-Turner, 1990, p. 12-13).

Aspects of Culture

The following section comes primarily from Kiely in Allen (ed), 2006, Wiley, in press).

There are six dimensions of culture that are especially relevant to security issues. These include:

1. Rules and Norms: Norms are deeply held assumptions that turn into repetitive attitudes and behaviors. Social Scientist Susan Shimanoff observed that groups of people who share a culture or sub-culture seem to have sets of unwritten rules--rules that are so imbedded in their culture that they cannot even articulate them, let alone see them objectively. (Kiely, 2001) The bottom-line is that people in organizations watch how

others survive and thrive, and they emulate those same behaviors and over time they become norms. And norms may fall anywhere on the continuum between very productive and dysfunctional/dangerous.

According to Schein (1992), norms might be observed behavioral regularities, group norms, espoused values, formal philosophies, rules of the game, aspects of climate, habits of behavior, and perhaps shared meanings and root metaphors, all-powerful, all operating largely unexamined, all capable of enhancing or seriously threatening the security of an organization.

2. *Tolerance for ambiguity*: To be able to survive in the 21st century, the norms inside an organization need to be flexibility, resilience, and adaptability, especially in the face of rapid change. Culturally, however, these abilities are deep-seated and cannot be changed just by willing them to be so; in organizations tolerance for ambiguity appears all along the spectrum of low to high. Tolerance for ambiguity: "...refers to the ability to react to new, different, and at times, unpredictable situations with little visible discomfort or irritation. Excessive discomfort often leads to frustration and hostility...." (Harris and Moran 1993, p. 104).

High tolerance for ambiguity might cause slippage or mistakes; low tolerance for ambiguity might cause a system to be so rigid, it cannot adapt rapidly enough. The inability to see potential danger could occur in either case, but for differing reasons, calling for differing solutions.

3. *Power distance* in an organization refers to perceived authority and how clearly the levels are delineated. For example, the perception of power is not only in the organization chart design but also in the informal beliefs, norms and myths. Cultures who revere their "elders" or prefer military type command and control are called "high power differential" (HPD). Cultures who believe "all men are created equal," have strong norms regarding diversity and who "empower" their workforce would be considered low power differential (LPD). The power differential issue affects information flow as well as many other productivity issues

4. *The Politeness Norm* is one of the ways the High Power Differential plays itself out. It is a form of cultural etiquette or diplomacy closely related to the maintenance of "face." Never underestimate the need of individuals to "save face" or to keep from "losing face." Cultures that have a high power differential and a collectivist perspective have a strong politeness norm as well. An assessment of organizational politeness norms can be very revealing regarding vulnerability in the face of security issues. It isn't simply that people see security problems, but aren't speaking up. It might be that the politeness norm is so strong that people have stopped looking altogether.

5. *Context* refers to the need or lack of need for shared background in order to create meaning. High context cultures, cultures that require fewer words and depend on the shared experience of members to generate meaning, are by nature more homogeneous and have more shared history. Low context cultures tend to be more individualistic and

heterogeneous, with multiple histories that were not shared. There is no pre-programmed “memory of the system,” so it takes more information, more words to activate the system. The problem, of course, is that this “low context” increases the need for information handling, thereby increasing the mass and complexity of the system. The information must be explicit, verbalized, written down. Shared meaning and understanding take a lot longer and demand multiple explanations both verbal and in writing. These cultures are more verbal and rely more on words and symbols to explain ideas and concepts. There is more likelihood of misunderstanding here; nonverbal behavior takes on less meaning or is misinterpreted. There is more documentation in these cultures and the documents tend to be much longer.

As this context issue relates to security, the more we integrate heterogeneous cultures into teams of people who have to make collective decisions, the more low context we have to be. As we implement the proposed paradigm shift, we must be low context--at first. But eventually, to be maximally effective, we must consciously strive to become high context. This means sharing and discussing multiple similar experiences, sharing them in low-context verbal interactions, thus developing shared implicit codes. The more high-context a team can become (through initially low context shared experiences), the more trust can develop and the more leaders will be able to foster growing collaboration and cooperation. This is the best and most sustainable way to change the DNA in a system.

6. *Collectivist versus individualist* refers to the general mentality of the people in an organization regarding the “we” versus “me” perspective. Many books are being written today trying to help organizations get to the “we” perspective. To oversimplify, this means when we make decisions do we make them with a focus on what’s best for me and my career or what’s best for the group, or what’s best for the organization. Studies have shown that the more the organization’s mythos is that “we will be around forever,” or the more ambiguity and uncertainty there is in a system, or the less clarity of goal or purpose are situations where people will tend to make more self-serving choices.

Culture & Security Problems

Our research has shown that about 80% of the time, a productivity problem can be mapped directly to a system flaw, which manifests itself in the organization’s culture (Kiely, 2004). These cultural issues include: alignment problems (conflicting goals), attitude issues (complacency, fear, burn out, etc.), Decision-making (too cumbersome, too autocratic, etc.), influence issues (inability to get buy-in, difficulty moving things forward), innovation and creativity, personnel, productivity), and so on.

In addition to the general list above, we have found a few other specific causes of system flaws (the interaction between organizational structure and the raw human resources) that should be mentioned here. 1) Some are caused by surgically treating specifics (perhaps only symptoms) rather than treating the system holistically. 2) Other causes relate to constant restructuring, the trendy, new thing to do to enhance productivity; it can lead to high levels of uncertainty and low levels of loyalty to people. 3) Another problem area is often the performance review and reward system. If not designed to enhance

performance and to appropriately and objectively reward it, we will get the path of least resistance. Many organizations today do not have a performance review system or an HR system that is aligned with organizational goals or appropriate performance.

Potential Solutions: the “Intentional Culture”

Returning to the concept of the “Intentional Culture”, we propose actually creating a culture within the organization in which people want to and are able to protect the entire enterprise, a culture where people automatically think in terms of what information to share and what to protect (See Kiely, *Creating the Intentional Culture*, 2006). This means that changes need to be instilled at the deepest level, into the DNA of an organization.

Homogeneous, high context, collectivist cultures with high power distance and low tolerance for ambiguity might be more rigid in their norms and perhaps less “modern,” but that does not mean they are less able to change. The more flexible, diverse, empowered, individualistic, and nimble we are might actually make it harder to create sustainable changes. That means we have to attack this at the level of the DNA—the norms, beliefs and attitudes not just behavior.

As far as diversity goes, we have programs on valuing diversity and differences, building tolerance, acceptance, and sensitivity. There are also hundreds of instruments in the marketplace that test personalities, styles, strengths, learning styles, etc. All of these tools are meant to create an understanding of human differences in order that we might collaborate more effectively and be more productive. It isn’t that simple however. As early as the 1970’s, Walter Mischel found that people with diverse personalities or values, etc. would exaggerate their differences in ambiguous, uncertain, or high threat environments. He also found that if we created situations that had strong parameters, people’s differences would diminish or at least weaken. The situational constraints he suggests are the following:

1. Knowledge of what one is supposed to do
2. The skills enabling one to perform appropriately
3. Knowledge of the outcomes
4. Knowledge of the rewards

Although these may seem intuitively obvious, they can be difficult to implement, and must be considered as long-term, sustainable goals toward creating a culture committed to security.

Briefly, some suggestions about what this will take:

- Provide people the knowledge, skills, and understanding of outcomes and rewards that Mischel suggests.
- Develop consistency of processes and protocols for information sharing and protection such as Six Sigma (or simpler variations) that people trust and train people, then hold people accountable for these protocols

- Give people disciplined “voice”, such as corporate dialogue programs, workout programs, etc.
- Create behavioral standards (both in reward and consequence) regarding how mistakes and breaches are handled
- Develop internal oversight groups (see “Governance” section)
- Externally (See Mitroff, *The Futurist*, 2005):
 - Make our oversight agencies stronger
 - Develop smarter regulatory agencies, not bigger ones
- Develop scenario training to change beliefs and attitudes.

For more on the subject of Building Intentional cultures, renorming, and mediated communication in virtual environments, or measurement see Kiely, *Building Intentional Cultures*, Libertas Press 2006 release.

An organization’s culture can be enlisted, re-defined, re-normed, and brought into the mix as part of the solution, rather than allowing it to be the problem. But in this discussion we have seen that it is an enormous issue and task, not to be treated simplistically, and full of potential for worsening our security and safety if we fail.

Call to Action:

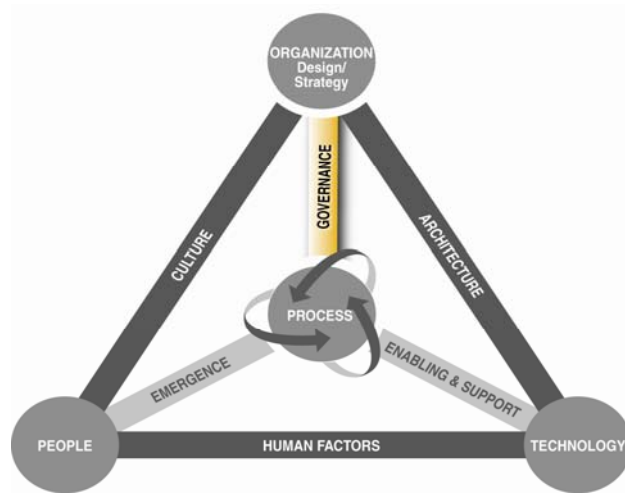
We invite discussion about these issues

Case Studies

Additional Readings

The Tensions, cont'd...

GOVERNANCE



A rising tide lifts all boats
--anon--

As we have seen, security breaches and harm to organizations can include damage to life, property, reputation, knowledge, data, or intellectual property, and are motivated, sometimes accidentally, sometimes by a lack of knowledge or neglect, and sometimes by actual intention to do harm. Threats must, then, be viewed through the lens of both organizational and national governance. Just as Colley et al (2003) have shown, the territory of security will eventually be occupied and addressed by both. It may be to our disadvantage, however, if the federal government steps in to determine the solutions to security issues. Prior to the passing of more stringent security policies by the national government, we do have a small window of opportunity to choose how organizations and government can optimally interact. It is this opportunity that motivates and calls for SSM.

Organizational Governance

We start this section by looking at organizational governance. To begin with an observation: notice how, when something awful happens in an organization, the people deeper in the organization are held responsible for the event? This usually happens due to the flawed interaction--the “tension” between the nodes of “organization” (which we remind you means strategy and structure) and “process” (which means policies and procedures). From a “strategy” point of view, this shows a need for a different approach. Security must be written into and embedded in the organization’s structure. For example, individuals deeper in the organization or human resources departments or IT groups cannot be held accountable for security. It must be adopted as strategy, made part of a high level policy and accountability, monitored at the highest levels of the organization.

In terms of “structure,” if security is housed in only one part of the organization or in the hands of only a few, the “process” is owned by them and the structure is designed to hold only that group accountable for anticipating, finding, or fixing security problems. By its very nature, this places responsibility deeper in the organization, not in the hands of the leadership. Structurally, where security is actually housed creates the tension between organization and process. We call that dynamic tension the organization’s “governance.” (As a reminder, by “tension” we mean the potential problems and/or the potential solutions most likely rest here).

A “cultural” look at the issue calls for the same answer. Of course the governance in an organization has a profound effect on the culture of that organization. Dozens of examples in both private and public sectors show that effective boards significantly influence the success of an organization and poor boards or boards who do not understand their role, can seriously damage the long term effects of success. To put it bluntly, the 21st century demands strategic leadership and the responsibility and accountability for security must be placed directly in the hands of the Boards and the collective C-suite executives.

But, as in all decisions of this magnitude, it isn’t quite that simple. Unintended consequences might cause even larger problems. For example, there is the ever-present cultural tension between the leaders micro-managing or being too hands-off. So the solution lies, not in handing security off to a group, or micro-managing a group to oversee security, but in having the board and the C-Suite executives build security into their job descriptions and their accountabilities as a part of governance.

As Colley, et al (2003) note, everybody knows that the responsibility for governing the affairs of a corporation lies with the board of directors. But what has not been resolved as an issue of *governance*, rarely even written about, let alone solved, is *where is security?* We think the answer should be: it should be made to rest with directors and their direct operatives, the C-suite executives.

Rationale for Security as a Governance issue

Following Colley’s discussion, governance (which is driven from the board and the C-suite executives) is supposed to:

- Align the actions of the individual parts of an organization toward aggregate mutual benefit,
- Provide the means by which each individual part of the organization can trust that the other parts each make their contribution to the mutual benefit of the organization
- Provide a means by which information can quickly flow between the various stakeholders to ensure that the changing nature of both the stakeholder needs and desires and the environment in which the organization operates get effectively factored into decision processes.

- Ensure that conditions apply whereby a firm's directors and managers act in the interests of the firm, its shareholders, and its workers
- Ensure that the means exist to hold managers accountable to investors and employees for the use of assets

This seems to imply the board's involvement in security, but it isn't explicit. We would add to Colley's recommendations the explicit provision that governance officers (board members and executives) must be required to provide strategies and protocols for the protection and preservation of the organization. This means the Board and the C-suite Executives would be held responsible for preservation and protection, as well as overall success.

Governance used to be defined simply as how well a board helps an organization accomplish its purpose. This consisted of choosing executive officers, advising and assisting in decisions regarding the selection of executive officers, business strategies, overseeing results, etc. Because of the events in the last decade, this "job description" is no longer enough. At best, this implies that the board will only secondarily oversee the well being of the organization; at worst, it means that the protection and preservation of the organization are not under the purview of the board at all. Whether the intention was one or the other, it simply isn't enough any more. *Governance must now mean equally the progress and success of the organization as well as its protection and preservation.*

This expanded role of the board needs now to be defined as to how effectively it protects the enterprise while simultaneously helping the organization accomplish its purpose. This re-defines the concept of *oversight*, which is no longer about simply building shareholder value in the short term, quarter by quarter. Today, with security in mind, oversight is now about long-term sustainability-- protection as well as progress. To be brutally clear, we are talking here about *governance*, not IT departments or divisions. We are talking about the top. In order that the preservation and protection of the enterprise must be housed in all areas of the organization's structural chart, the security "buck" must stop only at the top.

Recommendations

If the above is accurate, this means we must revisit the roles of Board members and Executives, how they are selected, and how they are held accountable. But the issue has larger implications because it involves the tension between Big "G" Government and small "g" governance.

Our pattern in the US has been to create new laws and restrictions reactively—like closing the barn door after the horse gets out. As a result of such debacles as Enron and Arthur Anderson and the new laws such as Sarbanes-Oxley, we have made some progress toward shifting the way we view and populate boards. Conflicts of interest and transparency are two of the areas where scrutiny has increased. But this is not enough; we need to find other ways to ensure the rigor of board selection and behavior. We could wait until another disaster forces new security laws, or we can learn from our past and

create new protocols that will preempt the need for new “laws” from national government. National legal restrictions as solutions to organizational problems have several draw-backs: 1) they tend to be local not global in reach and may not be respected or even recognized internationally; 2) They take too long to enact and are often poorly defined when they are passed; 3) They are often very disruptive and consequently very costly; 4) They are often defined by politicians who are interested in furthering their careers without input from the people who actually know the businesses that are affected; and 5) There is rarely an exit strategy from these laws.

On the other hand, if organizations who work with one another in the value chain or the value cluster demand of each other greater rigor and standards in security and governance issues, it may be possible to operate effectively using a philosophy consistent with the free-enterprise model. Self-regulation that produces added competitive advantage and brand equity is a beautiful thing. And, because very few organizations exist today that are purely local, what we propose here has at least cross-regional and national, maybe even global implications. Programs and standards that are emergent and self-regulating are far preferable to imposed legal constraints, and have the added advantage of sustainability even among states or countries with divergent legal approaches.

The names and reputations of corporate board members have often been used as a competitive advantage in corporations. Also, holding suppliers and vendors as well as customers to industry-defined, self-regulated, higher standard has successfully been used to create advantage. If we combine these two ideas, changing the standards of selection criteria for board members and executives can ensure that a criterion-based, not just reputation-based selection of board members or advisors enhances the organization’s success and social capital. This would require much more than a simple mind-shift on the part of boards and their non-corporate counterparts. It implies more of a paradigm shift. At a minimum, the shift would include the following:

- Understanding the criticality of security issues on the part of organizations, shareholders, stakeholders and potential governance officers
- A different attitude on the part of individuals who are in a governance role regarding their role and duties
- A new type of development, education, and training for people in governance positions that would be required as part of the new self-regulating standards
- Emergent, cross-industry communities of interest and communities of practice who could develop such criteria
- Criteria implemented corporation-by-corporation and holding vendors and suppliers accountable for implementing these standards internally. This paradigm shift model is similar to the TQM model rather than the Sarbanes-Oxley model. Government demanded TQM standards from its vendors thus raising the bar for all industries.
- Other requirements of the board:

- Clear understanding of what assets (both tangible and intangible) are potentially at risk, what the risks are and what mechanisms are in place to protect the entire enterprise.
- Clarity regarding the relationship between the board and management in security responsibilities
- Comfort on the part of the board that management has the ability to make decisions regarding prevention and protection of the enterprise
- Redefinition of the “Duty of Care” responsibilities to include board members’ knowledge of and prudence regarding issues of potential harm or potential crises
- Redefinition of the “Duty of Supervision” responsibilities to include knowledge of and prudence regarding issues of potential harm or crises as criteria for choosing and placement of executives
- Threat assessment audits and implementation of an “audit” committee for safety and security in addition to and similar to current fiscal audit committees with neutral auditors
- New security knowledge and criteria for CEO selection, performance review, and compensation
- New criteria and standards set by the customer base and shareholders regarding the selection criteria of board members of potential vendors, suppliers, partners and alliances
- New CSO or CPO positions

Summing up Security and governance:

Greater understanding of the roles of structure, strategy and culture in the dangers and challenges ahead will get us nowhere; indeed will flounder on the rocks of inaction or ineffectiveness if governance fails to implement what we have learned. The sheer interrelatedness of security dangers and problems, the inherency of the problem throughout the formal (and more importantly, *informal*) structure of the organization, and the deeply cultural dimensions of security issues, all point to a need for boards and executives to step up to this issue. Security has “arrived;” it has risen to the level of the governance and must be aligned to organizational goals. It is perhaps the most pristine example of the Roman concept of the *sine qua non*: it is literally the case, “without this, nothing.”

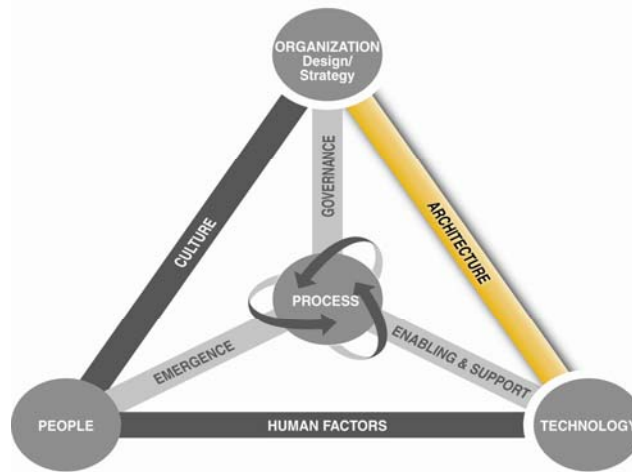
Call to Action:

We invite discussion about these issues

Case Studies

Additional Readings

ARCHITECTURE



Architecture is at the heart of the tension between the nodes of technology and organization. Without the connecting tension vector of architecture, technology and organization might seem to exist as independent islands. In fact, architecture is so important that our three-dimensional pyramid model would collapse without it. Analogously, an organization's information security cannot stand without a comprehensive architecture. In addition, not only does architecture provide the tension between technology and organization, but it also supports culture and human factors, as discussed elsewhere in this paper.

Security Architecture Defined

Security Architecture is a comprehensive formal encapsulation of all of the people, processes, policies and technology that comprises an organization's security practices. Often, Security Architecture is viewed as simply the relations between different technology components in an IT system. However, as we have shown throughout this paper, technology cannot stand on its own without integration into all other elements.

Architecture, as applied to information security, is the overall design or structure of a system typically described as the interconnection of hardware, software, and components that make up an organization's infrastructure. This is then complimented by the processes, policies and procedures that govern the practices. The more comprehensive an organization's security architecture is (that is, the more it includes all of the nodes and tension points) the higher the levels of systemic security an organization achieves.

Given the broad range of topics spanned, Security Architecture is often defined within a common framework that describes all of the components and provides a structure for

process and governance. The Network Applications Consortium (NAC) defines a policy-driven process for security architecture. As described by NAC:

It starts with defining an enterprise security program framework that places security program management in the larger context. It continues with in-depth focus on the three major components that make up enterprise security architecture: governance, technology architecture, and operations (2004).

Thus, Security Architecture provides a balanced relationship between strongly opposing elements and the interplay of conflicting elements and serves as a device for regulating tautness among an organization's governance, technology architecture and its operations.

Current Practice

The state of security architecture in current practice varies widely. Most organizations define technical security architectures but place little emphasis on organizational structure, people and operations. In order to address these shortcomings with a structural approach, there have been a number of efforts focused on defining security architecture frameworks. Generally frameworks are defined relative to specific domain needs; some of the best known are: SANS Information Systems Security Architecture for enterprises, the Department of Defense DoD Architecture Framework (DoDAF), and the Federal Enterprise Architecture Framework (FEAF).

The SANS (2005) enterprise architecture framework consists of 5 phases:

1. Security Assessments to determine security requirements
2. Security Architecture design based on recommendations reached in the assessments.
3. Development of security policies and procedures
4. Implementation of target security architecture (technology) designs.
5. Integration of security practices through change management and project management methodology to introduce security as a process.

In the government arena there are two standard frameworks, one for the DoD and one for federal enterprises.

The DoD Architecture Framework (DODAF) is based on an IEEE Standard (IEEE STD 610.12, 19903), and provides guidance for describing architectures for both war fighting operations and business operations and processes. The DoDAF defines architecture in terms of three related views:

1. Operational View
2. Systems View
3. Technical Standards View (2003)

This framework is largely oriented towards providing tools and techniques for understanding, comparing and integrating systems and systems of systems and places a high degree of emphasis on interoperability. These are key points in critical inter-enterprise operations and have applicability outside of the DoD and in relationships between enterprises such as are found in e-commerce practices.

The Federal Enterprise Architecture Framework is based on the National Institute of Standards and Technology (NIST) model (1999). The NIST model is used with the federal government as a management tool that illustrates the interrelationship of enterprise business information and technology environments. The NIST model is a five-layered model. The FEAF expands this model to include eight drivers which are then captured in the following four levels:

Level I (the view from 20,000 feet) is the highest level of the Federal Enterprise Architecture Framework and introduces the eight components needed for developing and maintaining the Federal Enterprise Architecture.

Level II (the view from 10,000 feet) shows, at a greater level of detail, the business and design pieces of the Federal Enterprise Architecture and how they are related. Viewed horizontally, the top half of the Framework deals with the business of the enterprise, while the bottom half deals with the design architectures used to support the business.

Level III (the view from 5,000 feet) expands the design pieces of the framework to show the three design architectures: data, applications, and technology.

Level IV (the view from 1,000 to 500 feet) identifies the kinds of models that describe the business architecture and the three design architectures: data, applications, and technology.

The FEAF was developed by the Chief Information Officers Council which was established by Executive Order 13011, *Federal Information Technology*, as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal information resources. The Council and FEAF continue to evolve as a living reference document and should provide input to many enterprise security architecture efforts.

Call to action:

We invite dialogue and debate here

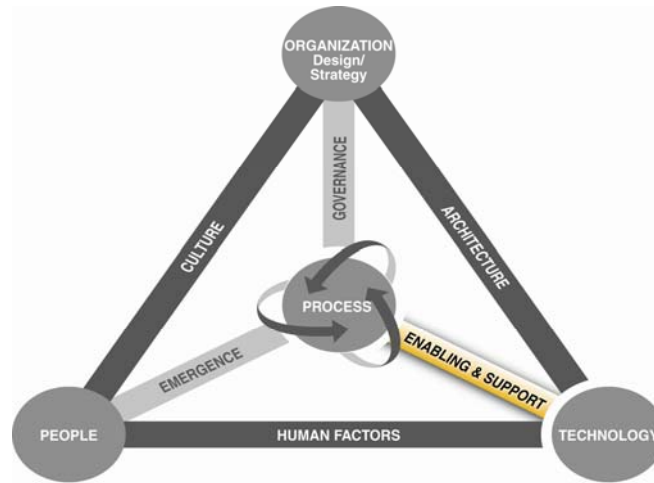
Case Studies:

Additional readings

- Network Applications Consortium NAC is a consortium of IT end-user organizations representing combined revenues of over \$800 billion, more than 55,000 network servers, and more than 1 million workstations
- <http://www.netapps.org/techpubs-esaexecsumm.html>
- From the *Executive Order on Critical Infrastructure Protection*, George W. Bush, The White House, October 16, 2001
- <http://www.sans.org/rr/whitepapers/auditing/1532.php>
- http://www.defenselink.mil/nii/doc/DoDAF_v1_Volume_I.pdf
- https://secure.cio.noaa.gov/hpcc/docita/files/federal_enterprise_arch_framework.pdf

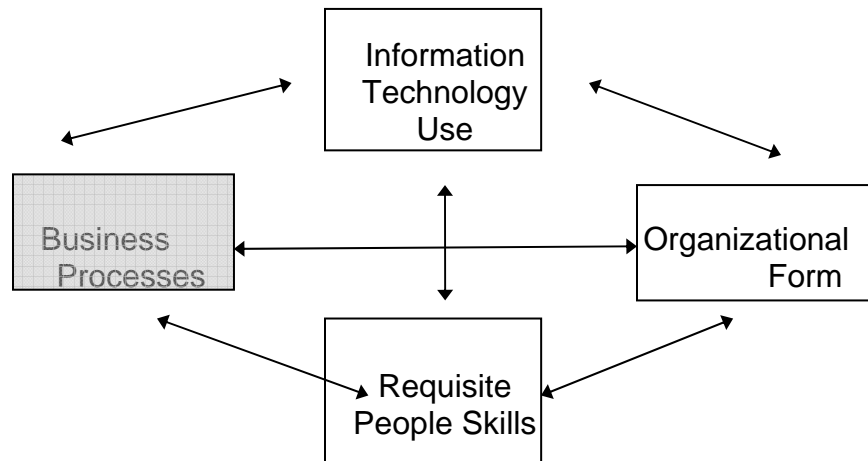
The tensions, cont'd...

ENABLING & SUPPORT



Traditionally, tension exists between the nodes of process and technology often because of budgets, legacy systems, a failure to align with new ways of doing things or growth. They are often found to be in opposition rather than synergistically working together. Between these two nodes the fundamental question is often whether the process is enabling the technology or is the technology supporting the process? A technology heavy organization with no supporting processes is at risk because it is not sustainable or extensible, and it is often disconnected from people, culture and processes. By the same token, an organization dominated by process may be lacking in supporting technology to implement the process and procedures necessary to complete an effective security systems. Examples abound from the complex to the simple. One simple example is when an organization implements “productivity” tools that are cumbersome and non-user friendly, but which are very secure. Or very friendly tools that are easy to use but not secure.

“Enabling and supporting” thus defines the holistically aligned relationship and connection between process and technology. Processes can be redesigned by changing their architecture and flows, by changing the information technologies that enable them, the organizational structure that houses them, and the people skills, incentives, and performance measures of the people who execute them (El Sawy, 1999, Chp. 3-3, figure 3-2) To assure achievement of systemic security it is important that all these interactions are taken into account in any IT initiative or process reengineering project.



("Leavitt's Diamond")
Factors that interact with Business Process Changes

Current Practice

There are three commonly recognized ways to use technology to enable the redesign of business processes (El Sawy, 1999, 3-4), not all of which actually enhance the security of the process. These are:

1. Restructure and Reconfigure the process. When done to enhance customization for customers and to streamline processes, care must be taken not to make the results so complex or unique that security becomes impossible to maintain.
2. Change information flows around the process. This approach greatly increases the amount of digital information that exists within the organization creating much more vulnerability to cyber security attacks, but also providing the possibility for a more enriched set of security systems that can bring added value to the process redesign.
3. Change knowledge management around the process. While this is often done to improve the performance of the organization through continuous learning systems, the knowledge generated can also be used to provide input to security processes that take into account all actors in the process, both those within the organization and those like suppliers or customers interacting with it.

Any business process can be redesigned by modifying the information flows around it so that information is captured as early as possible in digital electronic form. When this concept is applied to security processes, the possibilities for more real time information on potential security breaches are immediately apparent. But this type of linkage between process and technology also enables the process to take better advantage of the information for decisions to be made on such critical security issues as information sharing, identity management, and boundary management. As pointed out by Majchrzak

and Benzel, once information is digitized in electronic form, sophisticated artificial intelligence software systems can be used to enable superior functionality for the process as well.

While the possibilities for enhanced process performance through the introduction of information technology are great, once again a caution must be issued to continue to monitor the tension between the two nodes. For example, as El Sawy, Chellappa, and Griffith pointed out in their white paper on identity management for SIM (2004), the failure to design sufficient flexibility into such systems can often lead to users finding ways to work around the controls that the system is designed to put in place. If IDM systems parameters are “over-tightened” such that user procedures are excessively cumbersome, this may encourage not only user-initiated work-arounds, but enterprise-aware workarounds as well. The most common example of this phenomenon is the use of post it notes around every enterprise PC listing each password required for each application the employee needs to use. The difference in adherence to identity authentication between the appearance of Tom Cruise on the Paramount lot vs. the care taken to authorize an ordinary visitor is another example of the need to have flexibility in the technology supporting a process so that, for instance, IDM system parameters can be set differently for diverse stakeholder groups (customers, partners, employees) in order to preserve business value and security.

Recommendations

The solutions to these tensions rest in the emergent culture and cross-functional groups influencing each other and making collective decisions for the right reasons. Most organizations exist with isolated islands of organizational strategy, architecture, technology, and people, loosely coupled together with processes, governance, and organizational structure. To fully realize systemic security, Enablement and Support approaches must be used that provide sufficient flexibility, even in emergent environments, that the tensions can be resolved at the point of process execution and without the need to resort to rigid policy statements or hierarchical review. This means the roles of enabling and supporting functions, which often reside in IT divisions (note the irony of the word “division”) need to learn to be more consultative and facilitative in style rather than obstructionist. And, security must be one of the top criteria rather than buried under the criteria of current need, budget constraints, and legacy technology. (The related concept of “emergence” is discussed in the next section.)

Finally, to build a more stable and secure enterprise, implement the recommendations in this report and then add in additional care and emphasis to ensure that tensions are carefully monitored and adjusted on a regular basis.

Call to action:

We invite dialogue and debate here

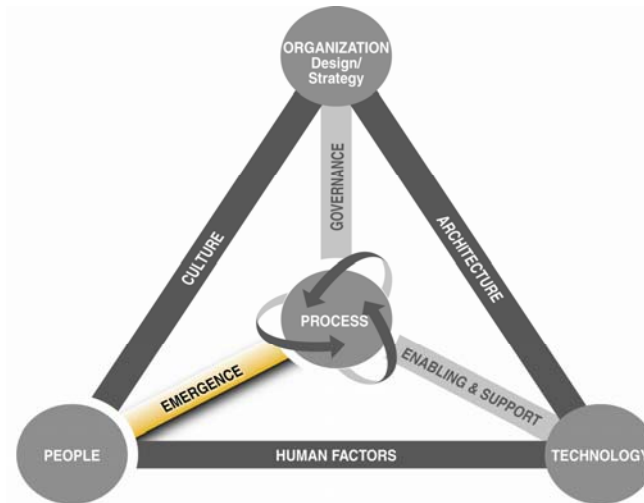
Case Studies:

Additional readings



The tensions, cont'd...

EMERGENCE



*“My concern for this country is that we are passing off as progress what is really just change, and rather than dispensing knowledge, we should be dispensing wisdom.”
--Abraham Lincoln--*

Our model has positioned “people” and “process” in such a way that “emergence” appears as a “tension.” There is good reason for this, reason to pay attention to the issue of emergent processes in security issues. By “emergent,” we refer to developments and patterns that arise in the course of our enterprise which appear to have no obvious cause, and whose outcomes seem impossible to predict and control. For example, emergence suggests that the exact nature of the trade-offs between sharing and security experienced by an individual engaged in the collaborative process cannot be known in advance. Thus, policies and procedures that specify in advance how an individual should act are both infeasible and likely to be ignored (Majchrzak, 2004). In fact, the word emergent implies a process that is inherently “not routine” and therefore not amenable to a top down approach to its management. To the extent that the new, the unpredictable, the emergent is a part of every organization; it becomes a major security concern and a potential place for solutions to occur.

“Tension” Between People and Process

People like predictability and are very willing to keep doing what they are doing especially if they believe the organization has decided on the best process or way to do things. Process, from its Latin roots, means movement. “It is a naturally occurring or designed sequence of operations or events, possibly taking up time, space, expertise or other resources, which produce some outcome.” (*Wikipoedia*) But a hamster in a wheel is moving. That might represent change, but not necessarily progress. Very often process

means the formal policies and procedures through which “stuff gets done,” with the result that we may get stuck in the same old process over and over again, creating a “loop” of behavior or perspective which does not change.

What we would hope our process would accomplish is *improvement*. Developing better ways to do things, benchmarking, best practices, balanced scorecards, lean thinking, better efficiencies and effectiveness, etc. The process itself may represent progress, but once implemented, might become repetitive to the point of entropy. For security this dulling of awareness due to repetition can be especially dangerous. On the other hand, if one pays attention to the non-routine or exception to the process, new ideas for improvement and new challenges to security often “emerge.”

Understanding Emergence; Developing SSM

The concept of emergence comes from many different fields. We borrow it here from fields such as systems theory, game theory, and Mother Nature. Chaos theory also explains the concept of emergence. In chaos or decentralized or leaderless situations, some type of order will emerge or surface seemingly unpredictably, and without obvious cause. To give it our working definition, emergence is a dynamic process of patterns occurring over time that seem not to be created by a single entity, person, event, or rule but rather from the activity itself. We especially love the *Wikipoedia* definition of emergence: “There is nothing that commands a system to form a pattern, but instead the interactions of each part to its immediate surroundings causes a complexity which leads to order. One might conclude that emergent structures are more than the sum of their parts because the emergent order will not arise if the various parts are simply coexisting; the interaction of these parts is central.”

Emergence means surfacing, developing, growing, or evolving. In previous business models it might have been called continuous improvement. Peter Senge called this “learning”. What we propose here is not entirely different from these models, but perhaps more like “thinking” organizations. Whereas resilience has been the catchword in the last few years, it is unfortunately reactive. Something happens, then we respond, bounce back. In our “emergence” idea, what we propose is not *reactive*—how long it takes an organization to bounce back after a crisis—but instead *proactive*. Being better at anticipating, building a culture that has enough faith in itself to allow emergent rather than prescribed processes and more importantly, outcomes. This is at the core of Systemic Security Management (SSM). A thinking organization is: “...a network of people, grounded in the learning process by not being constrained by what they know, who use value-based, future-focused inquiry to create, test, and implement new organizational practices.” (Logan, et al, 2002, p. 26.) This helps us learn to view every problem as if it were unique rather than repeats of where we have been before. It allows for being creative and perhaps even predicting surprises.

What we are proposing here is to recognize the “emergence” tension. Just because we have talented people and a rigorous process does not mean that we have an organization that is appropriately emergent, that is anticipating problems, dealing with them in

advance. If you recall, we earlier mentioned that not only do the interactions between nodes create tensions in our model, but the tensions must be balanced as well. It is here where you can see the dangers of the tensions being out of balance and affecting one another. In this case, the “emergence” tension and the “culture” tension directly affect one another. They are not one-and-the-same, however. Example: if an organization’s cultural values and norms include, “take care of each other and don’t confront,” there may be no positive tension, no provocation toward improvement or innovation.

So process isn’t the simple answer, and does not automatically lead into the emergent.

Harnessing the “Emergent”

Process programs are not enough to capture emergence. They can perhaps ensure critical thinking. This, in a successful organization, is called continuous learning or a learning organization. But process programs do not ensure a culture of creative thinking that can deal with emergent issues and environments. Being able to anticipate the future means a huge amount of innovation mixed into the recipe. An organization that focuses on the emergent tension is one that goes beyond learning to becoming a *thinking* organization and beyond resilience to being “*ready*.” (Kiely, 2007)

For example, many security challenges occur in environments that require collaboration and information sharing. The most vivid and tragic examples of this requirement are contained in the narrative of the 9/11 Commission report. Rather than prohibiting certain types of sharing or certain types of actions, as was the policy with the FBI, CIA and other security agencies in the federal government before that attack, emergence suggests that information security policies should emphasize keeping employees dynamically informed about potential security breaches that may result from their actions (Majchrzak 2004). Emergence also suggests that any security protection tool, policy, or procedure must be self-deploying and seductive, meaning that it must draw people into “doing the right thing”, sometimes without ever realizing it—something that would be hard to say about most non-systemic security practices today.

Emergence also implies that leaders of an emergent process are rarely appointed, instead they emerge. Thus, leaders who champion information security protection need to be encouraged to emerge, rather than appointed. Emergence also means that knowledge relevant to information security breaches will be distributed across individuals within an organization and across organizations. There need to be forums where information about breaches, fixes, and prevention can be shared (See culture section on High and low context). Finally, emergence suggests that people behave based on feedback rather than standard procedures. Thus, they need feedback on their work processes that encourage them to behave securely. (Majchrzak, 2004, p.4). In other words a thinking organization must be created whose fundamental process design celebrates and incorporates the concept of emergence.

Emergent Thinking

Emergent thinking must be a core competency of any organization in the 21st century. When it comes to security issues and survival, we must assume at all times that there are people out there who would do us harm and we must be prepared. This by no means asks you to go to the dark side. Optimism and skepticism can co-exist nicely. F. Scott Fitzgerald once said “The mark of a whole human being is the ability to hold two conflicting thoughts in one’s mind simultaneously and still be able to function.” Someone equally wise also said, “Just because you’re paranoid doesn’t mean they’re not out to get you.”

If security is to be achieved in our organizations and our lives, we need to develop a kind of preparedness, a climate based on our having covered all the bases of culture, people, structure, strategy and governance. And we need to reward our people not for a perseveration of old processes but for creating ongoing new ones, new ways to explore the problems to come, before they come.

Recommendations:

To ensure the strength of an emergent process and culture:

1. Create an organizational design that builds in process rigor, feedback loops, critical thinking, and creativity into daily practices
2. Use rigorous processes and innovative practices not only in terms of product, service, customer or organization purpose, but also in assessing potential liabilities and risks. Employ a group or teach each individual to look for sources of harm
3. Ensure the quality of the “process” node of the organization and the emergent nature of process improvement; create organizations that have:
 - a. Cultures that embrace improvement rather than resist it
 - b. Processes (not too rigorous, not too rigid) that build discipline into what gets done and how things get done.
 - c. Rigorous process improvement programs that will reinforce the strength of an organization and its protection as it learns
4. Ensure alignment with the “People” node; create organizations that:
 - a. Develop cultural norms that become part of the DNA of the organization; Some of this is done by:
 - i. Hiring appropriate resources
 - ii. Continuous training and development
 - iii. Applying appropriate performance review standards that are inclusive of the above
 - b. Ensure the innovation nature of “emergence;” create organizations that build innovation into the DNA of the culture by:
 - i. Changing the way decisions are made
 - ii. Focusing on the exception and not the rule
 - iii. Changing the culture to allow for disagreement
 - iv. Developing creative and innovative thinking in groups and individuals

- v. Ensuring that process improvement programs are one of the means by which we arrive at outcomes, not an end in themselves.
 - vi. Applying these tools and norms to the protection and security of the enterprise, as well as to other “emergent” new ideas.
5. Develop a group and individuals who are specifically focused on possible sources and means of harm
 6. Ensure that these behaviors are demonstrated consistently by senior executives and boards
 7. Build the above into all decisions, projects, etc.
 8. Expect and embrace radical emergence, not just the incremental emergence of continuous improvement.
 9. Establish governance policies that support and reinforce the above both in attention and budget

Call to Action

We invite discussion here

Case Studies

Additional Readings:

- Predictable Surprises by Bazerman and Watkins

THE SYSTEMIC SECURITY MANAGEMENT MODEL

American Center for Strategic Transformation, Steve Rayner, Bill Belgard and ICIIIP's Charles P. Meister and Phil Cashia *Five levels of Security Continuum* <http://www.marshall.usc.edu/ctm/ICIIIP/Graphics/Security%20Matrix%20ICIIIP%205%20Levels.pdf> have created a test by which to assess where your organization fits in the continuum toward SSM. Ask yourself which of the following models best describes where you are currently. Then go back over the sections of this paper to determine where you need to focus your attention in order to get to the next level toward SSM.

Level 1. *Functional Focus* relies primarily on sophisticated technology to maintain a secure workplace with most security personnel working 'behind' the scenes. Virtually all security issues are handled by the security personnel. There is little involvement by senior management in security related issues except in the event of a security breach.

Level 2. *Integration Focus* has the security department primarily responsible for control access, theft prevention and crime at the work place. The security function recommends policy and process changes to site management. Security recognizes the importance of gaining acceptance and compliance when introducing new protocol. The security function tends to operate secretly. Managers see limited business benefit to the security function and are often frustrated by policy and rules that interrupt the natural flow of information and material.

Level 3. *Communication Focus* has the security function sharing relevant information with groups and departments where they have identified potential problems. The intent is to communicate information with managers only when they have identified potential problems to increase overall awareness. The flow of information is one way, with security professionals reinforcing policy, describing security incidents, and informing people as to how to prevent their recurrence.

Level 4. *Commitment Focus* has all employees receiving training that has versed them in potential security threats and the direct actions they should take when confronted with a breach in the security system. The security function regularly shares information with employees about security performance and how it can be improved. The security function works jointly with managers and non-managers to determine the most effective combination of technology and employee diligence.

Level 5: *Systemic Security Management (SSM)* is a management approach to security which serves not only the enterprise but also the extended enterprise, going well beyond the boundaries of the company to include people, process, technology and organization as well as partners, suppliers, and customers. The direct involvement of upper level management and the board in overseeing the systemic security system has created a set of enterprise-wide values, ethics and cultural norms in alignment with their desired view of the future. Security is built around a set of core principles whose intent is to ensure an optimal balance between protection and the ability to share information and develop innovations among strategic partners to do business in a highly integrated way while

ensuring that digital assets, intellectual property and proprietary technologies are protected and secure.

<http://www.marshall.usc.edu/ctm/ICIIP/Graphics/Security%20Matrix%20ICIIP%205%20Levels.pdf>

You will notice that Level 5 extends the perspective beyond the internal workings of an organization into the larger external environment which must include customers, vendors and suppliers, partners and alliances, competitors, the industry at large, and so on. Although we have made reference to external contingencies (see section on governance for example), we have not covered the external issues in this document. That is because of our announced micro-to-macro approach. You might call it the “get your own house in order first” approach, which, as we have noted is very consistent with the philosophy of free enterprise. This paper, we would remind, is intended to start a dialogue. And speaking of “emergence” as one of the important tensions of the SSM Model, we look forward to and invite that which will surely be “emergent” in this discussion, the new thoughts and debate to come on the ideas we have presented here. And while that discussion continues we will be moving toward the next step, developing a document to stimulate some debate and dialogue as to how these issues play out in the national forum, and further, the global stage.

CONCLUSION

So we have discussed the four nodes of the pyramid: Organizational Design and Strategy, People, Process, and Technology. These nodes are connected through “tensions” that need to be finely tuned and rigorously watched lest they go out of balance. We have argued that much of the peril regarding security is housed in these tensions. We have also argued that the solutions probably rest there as well. Our recommendations are a preliminary proposal to which we hope the great minds will add content and debate.

Specifically we have suggested:

1. Understanding the interconnectedness of the parts of the ICIIP SSM model
2. Putting protection and preservation at the same level as progress and profit
3. Building protection and preservation behaviors into the design and strategy of the organization
4. Creating a new focus on security issues as they relate to recruiting, placing, and managing personnel
5. Increasing the emphasis on information security technology and identity management
6. Including protection and preservation of the organization in all formal processes
7. Paying close attention to the human factors that are caused by the interaction of people and their actual use of technology
8. Knowing that most of the problems and solutions for security issues lie deep in the DNA or cultural level of an organization, in its informal and implicit processes, and that this tension is brought about by the interaction of people and the way the organization is designed and what it states its purpose and direction to be.
9. Housing the responsibility for security of all tangible and intangible assets and their oversight and governance with the Board of directors and the C-suite executives
10. Architecting the technology and its use to be aligned with the organization’s design and strategy (which now include protection and preservation as well as progress)
11. Creating and developing the resources which can enable and support the new focus on security and the technology and architecture that are necessary for ensuring a safe environment.
12. Using emergent methods to ensure not only “learning” organizations but more importantly “thinking” organizations.
13. Recognizing that this is more of a dynamic process than a linear model. Constantly circling back to balance the tensions and maintaining eternal vigilance is critical.

Bummer. Security is no fun, a real downer. We mourn the loss of innocence that has caused the need for this paper. And while we wax realistic and look at the bad news without flinching, and while we muck around in the possibilities of terror, destruction, loss of life, hatred, revenge, and madness, doing our best to fight off the bad guys, let us

remember *balance*, remember that we fight this fight in order to preserve and enjoy that which is beautiful and good in our enterprises. And above all, we continue to thrive under the influence of the civil liberties that we treasure, taking great care not to destroy them through the very measures we are taking in order to protect them.

Having said all that, we must accept that the age of our innocence is indeed past. We are now keenly aware of how fragile our systems are, how vulnerable they are to attack or simple neglect or just looking the other way. It is the age of vigilance and preparedness and scrutiny. Like it or not, that ship has sailed, and we are either on it or we're waving goodbye.

REFERENCES

American Center for Strategic Transformation and [ICIIP's Five levels of Security Continuum](http://www.marshall.usc.edu/ctm/ICIIP/Graphics/Security%20Matrix%20ICIIP%20%20Levels.pdf)
<http://www.marshall.usc.edu/ctm/ICIIP/Graphics/Security%20Matrix%20ICIIP%20%20Levels.pdf>

Barton, L. *Crisis in Organizations*. Cincinnati: South-Western Publishers, 1993.

Cameron, K. S., and Quinn, R. E. *Diagnosing and Changing Organizational Culture*. Reading, Massachusetts: Addison-Wesley, 1999.

Colley, J. L., Doyle, J.L., Stettinius, W., and Logan, G. *Corporate Governance: The McGraw-Hill Executive MBA Series* New York: McGraw Hill, 2003.

Department of Homeland Security, [“The National Strategy to Secure Cyberspace”, Threats and Protection, Critical Infrastructure](http://www.whitehouse.gov/pcipb/), 2003.
<http://www.whitehouse.gov/pcipb/>

DODAF: DoD architecture framework working group, “DoD Architecture Framework- Version 1.0”, August, 2003.
http://www.defenselink.mil/nii/doc/DoDAF_v1_Volume_I.pdf

El Sawy, O. Redesigning Enterprise Processes for e-Business, December, 1999, Chapter 3 - 20.

El Sawy, O., Chellapa, R., Griffith, T.: Designing Identity Management for Business Value, Final Report for SIM Advanced Practices Council, December, 2004.

Farah, G. [“Information Systems Security Architecture: A Novel Approach to Layered Protection”](http://www.sans.org/rr/whitepapers/auditing/1532.php), *Sans Infotech Reading Room, Auditing and Assessment*, January 22, 2005
<http://www.sans.org/rr/whitepapers/auditing/1532.php>

[FEAF Federal Chief Information Officer \(CIO\) Council, Federal Enterprise Architecture Framework \(FEAF\). Version 1.1, September 1999.](http://www.cio.gov/archive/bpeaguide.pdf),
<http://www.cio.gov/archive/bpeaguide.pdf>

FFIEC, [“Information Security: IT examination handbook”](http://www.ffiec.gov/ffiecinbase/booklets/information_security/information_security_1ow_res.pdf), Published on
http://www.ffiec.gov/ffiecinbase/booklets/information_security/information_security_1ow_res.pdf, 2002

Galbraith, J. R. *Designing Organizations* (Second Edition). San Francisco: Jossey-Bass, 2001.

Hall, E.T. *Beyond Culture*. Garden City, New York: Anchor Press/ Doubleday, 1976.

Hampton-Turner, C. *Creating Corporate Culture*. Reading, Massachusetts: Addison-Wesley, 1990.

Harris, P. R. and Moran, R. T. *Managing Cultural Differences*. Houston: Gulf Publishing, 1993.

Hofstede, G. *Culture's Consequences; International Differences in Work-Related Values*. Beverly Hills: Sage Publications, 1984.

Hofstede, G. *Cultures and Organizations; Software of the Mind*. New York: McGraw Hill, 1991.

ICIIP, "Five Levels of Security: An Overview", American Center for Strategic Transformation, 2004.

Kiely, L. "Corporate Universities as Shapers of Culture", In M. Allen (ed.), *Advances in Corporate Universities*. Wiley, 2006 (in press).

Kiely, L. "Navigating the *Real* Final Frontier," *ACPE Journal*. January, 2004.

Kiely, L. *Creating the Intentional Culture*. Los Angeles: Libertas Press, in press 2006 release.

Kiely, L. "Measurement in Corporate University Learning Environments: Is It Gonna Show? Do We Wanna Know?" In M. Allen (ed.), *The Corporate University Handbook*. New York: Amacom, 2002.

Kiely, L. *Ready!?!?!?*. Los Angeles, Libertas Press, in press, 2007 release.

Kiely, L. S. "Overcoming Time and Distance: International Virtual Executive Teams." In Mobley, W. H. and McCall, M. W. (eds.), *Advances in Global Leadership*. Amsterdam: JAI, 2001.

Logan, D., Kiely, L. and Greer, J. "Beyond Learning Organizations: Building an Organization that Thinks," *Across The Board*, 2002.

Majachrzak, A. "[Human Issues in Secure Cross- Collaborative Knowledge – A Conceptual Framework for Understanding Issues and Identifying Critical](http://www.marshall.usc.edu/ctm/ICIIP/Documents/Ann%20Majchrzak%20Human%20Issues%20in%20Secure%20Cross%20Enterprise%20Collaboartive%20Knowledg%20Sharing%20White%20Paperat%20USC%20%20041504.pdf)", ICIIP White Papers, April 15, 2004.
<http://www.marshall.usc.edu/ctm/ICIIP/Documents/Ann%20Majchrzak%20Human%20Issues%20in%20Secure%20Cross%20Enterprise%20Collaboartive%20Knowledg%20Sharing%20White%20Paperat%20USC%20%20041504.pdf>

McCarthy CompTIA,
http://www.comptia.org/about/pressroom/get_pr.aspx?prid=611

Mitroff, I. "Crisis Learning: The Lessons of Failure," *The Futurist*. September 1, 2002

Mitroff, Ian, I. 2004
<http://www.marshall.usc.edu/ctm/ICIIP/Documents/Ian%20Mitroff's%20Vulnerability%20Management%20for%20Enterprises%20White%20Paper.pdf>

NAC, "Enterprise Security Architecture: A Framework and Template for Policy Driven Security", Position paper published on
<http://www.netapps.org/techpubs.htm#positionpapers>, 2004.

Report to the President: Cybersecurity a Crisis of Prioritization:
http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

Ranum, M. J. "An Internet Firewall," *World Conference on Systems Management and Security*, 1992.

Schein, E. H. *Organizational Culture and Leadership* (Second Edition). San Francisco: Jossey-Bass, 1992.

Wikipoedia. On-line reference guide.

Yakabovicz, E. P. "IDS and IPS: Information Security Technology Working Together," Guest Commentary on Security Tips, Published on www.techtarget.com, 2003.

LAREE S. KIELY, CPT, PH.D.

Laree Kiely, Ph.D., CEO of the Kiely Group--Organizational Effectiveness Consultants--has over 25 years' experience consulting, researching, and teaching organizational behavior to businesses internationally.

She served as a faculty member of the Marshall School of Business at the University of Southern California for 15 years, where she taught in the MBA and executive education. Prior to her appointment at USC, she directed Technology Services at First Interstate of California. She received Her B.A. and M.A. from the University of Colorado and her Ph.D. from the University of Southern California.

Dr. Kiely is the recipient of several teaching awards including the “Best Corporate Intervention” award from the International Society for Performance Improvement; USC Marshall School of Business "Golden Apple" Award for Teaching Excellence; and her course on "Negotiation: Plays, Ploys, and Pitfalls" was granted the Best Distance Learning Program for Corporate Development from IDLCON.

In addition to several papers and articles on business issues, Dr. Kiely is the author of *Creating the Intentional Culture*; “Navigating the *Real Final Frontier*” in the *ACPE Journal*; “Measurement in Executive Development: Is It Gonna Show, Do We Wanna Know?” in *The Corporate University Handbook*, Amacom Press 2002; “Overcoming Time and Distance: International Virtual Executive Teams” in *Advances in Global Leadership*, Volume 2, JAI 2001; and co-author of *Taking Charge: A Guide to Personal Productivity*, Addison-Wesley 1991, and *Everything’s Negotiable*, Amacom Press (Re-release 2005).

You can see her award-winning television series, *Tools for Leadership*, regularly on PBS.

TERRY BENZEL

Terry V. Benzel is Deputy Director for the Computer Networks Division at the Information Sciences Institute (ISI) of the University of Southern California (USC). She participates in business development, technology transfer and special projects with industrial and academic partners. She is the technical project lead for the Cyber Defense Technology Experimental Research (DETER) test bed and associated Evaluation Methods for Internet Security Technology (EMIST) research projects, jointly funded by NSF and DHS ARPA. The combined project is developing an experimental infrastructure network and scientifically rigorous testing frameworks and methodologies to support the development and demonstration of next-generation information security technologies for cyber defense.

Ms. Benzel has a joint appointment at the Marshall School of Business where she is a researcher at the Institute for Critical Information Infrastructure Protection. She is responsible for helping to develop Systemic Security Management as an open source body of work and developing public/private partnerships in information security research.

Prior to joining USC ISI, Ms. Benzel was a Division Vice President at Network Associates, Inc. where she was responsible for all aspects of the 125-staff advanced research organization performing government funded R&D for DARPA and other agencies.

Ms. Benzel has served as an advisor to government and industry on R&D strategy and roadmap development, providing guidance to White House Office of Science Technology and Policy, Critical Infrastructure Assurance Office, Department Of Defense and industry alliances. She testified before House Committee on Science, “Cyber Security –How Can We Protect American Computer Networks from Attack: The Importance of Research and Development”.

Ms. Benzel holds bachelors and master’s degrees in mathematics from Boston University and an Executive MBA from UCLA.