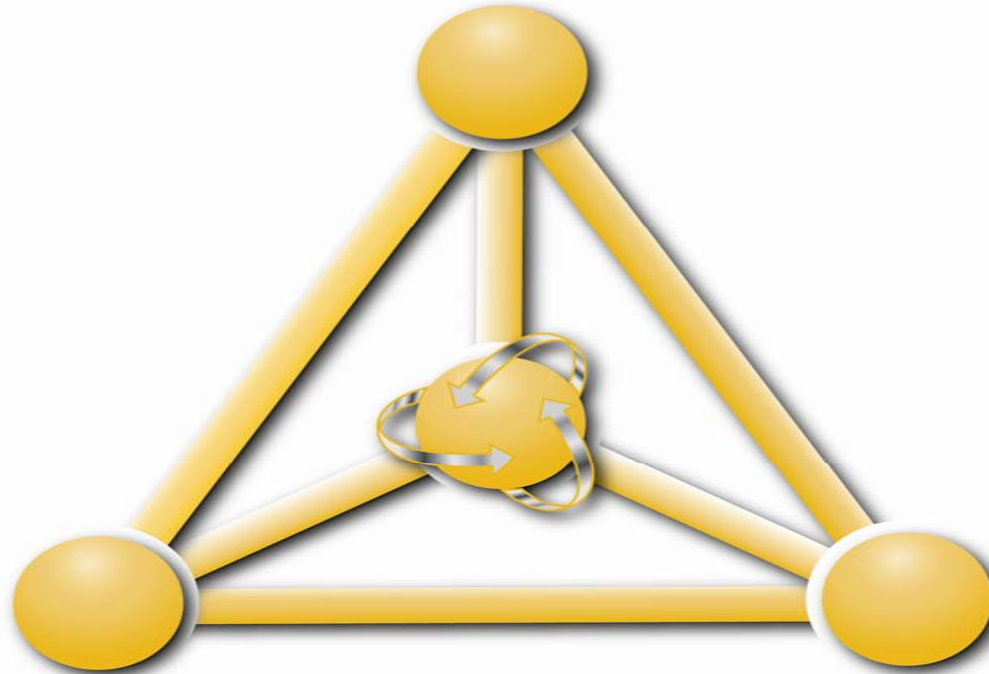
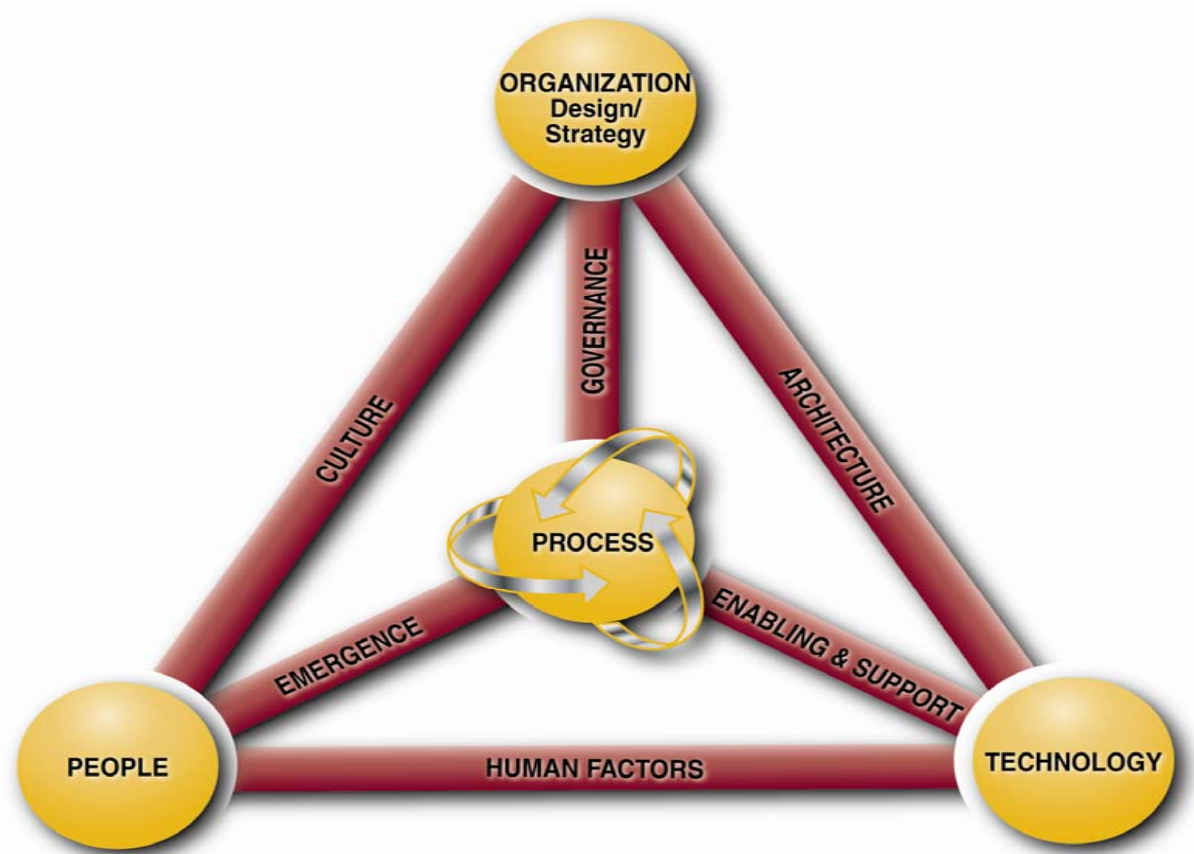


Systemic Security Management: The ICIIP Model



Laree Kiely, Ph.D. and Terry Benzel

The ICIIP Model



Defining Security

- A real or potential compromise of safety/security and/or damage to tangible (life, limb, property, data, money) and/or intangible (goodwill, credibility, reputation, knowledge, relationships, social capital, knowledge capital) assets
- May be systemic, internal, and/or external; intentional or unintentional or in combinations of the above

The Nodes: Organization Strategy and Design

Strategy Definition:

- An organization's formula for successfully accomplishing its *raison d'être* or purpose (Profit and non-profit)
- The basic direction of the company
- The goals and objectives to be achieved as well as the values and missions to be pursued
- The products or services to be provided, the markets to be served.
- The value to be offered to the customer

The sources of competitive advantage and ways to provide superior value." (Galbraith, 2001)

Strategy Recommendations:

- Develop a strategy for preservation as well as progress.
- Add a *preservation* statement to the purpose statement
- Inform and educate all as to this dual purpose
- Each individual and unit must demonstrate alignment with both the purpose and preservation standards.
- 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, 2006)

Design/Structure Definition:

- The “Org Chart”
- The placement of power and authority
- Oversight of security is often diffused among many “boxes” deeper in the organization chart

Recommendations:

- Design orgs to protect the the strategy system-wide
- Place oversight and coordination at the highest levels
- Security must be housed in the c-suite: Consider perhaps a CPO or CSO.

The Nodes: People

People Definition:

- The human resource policies of recruiting, selection, rotation, training and development.
- The talent required by the strategy and structure of the org
- The skills and mind-sets necessary to implement the chosen direction
- The organizational capabilities needed to execute the strategic direction
- Compromises to safety and security, whether intentional or unintentional, almost always involve people either as cause or effect or sometimes both.

People Recommendations:

- Job Descriptions; Recruiting and Selection; Placement and Rotation
- Skills, training, and development
- Reward systems and HR policies
- Performance feedback
- Physical placement of human resources

Cautions/Recommendations:

- Stifling the free flow of information can paralyze
- “Better security” can become “Unable to produce.”
- All employees and stakeholders must be system “ecologists”
- Self-regulating systems are preferable over new federal laws.

• We must be careful not to destroy the very liberties we are seeking to protect

The Nodes: Technology

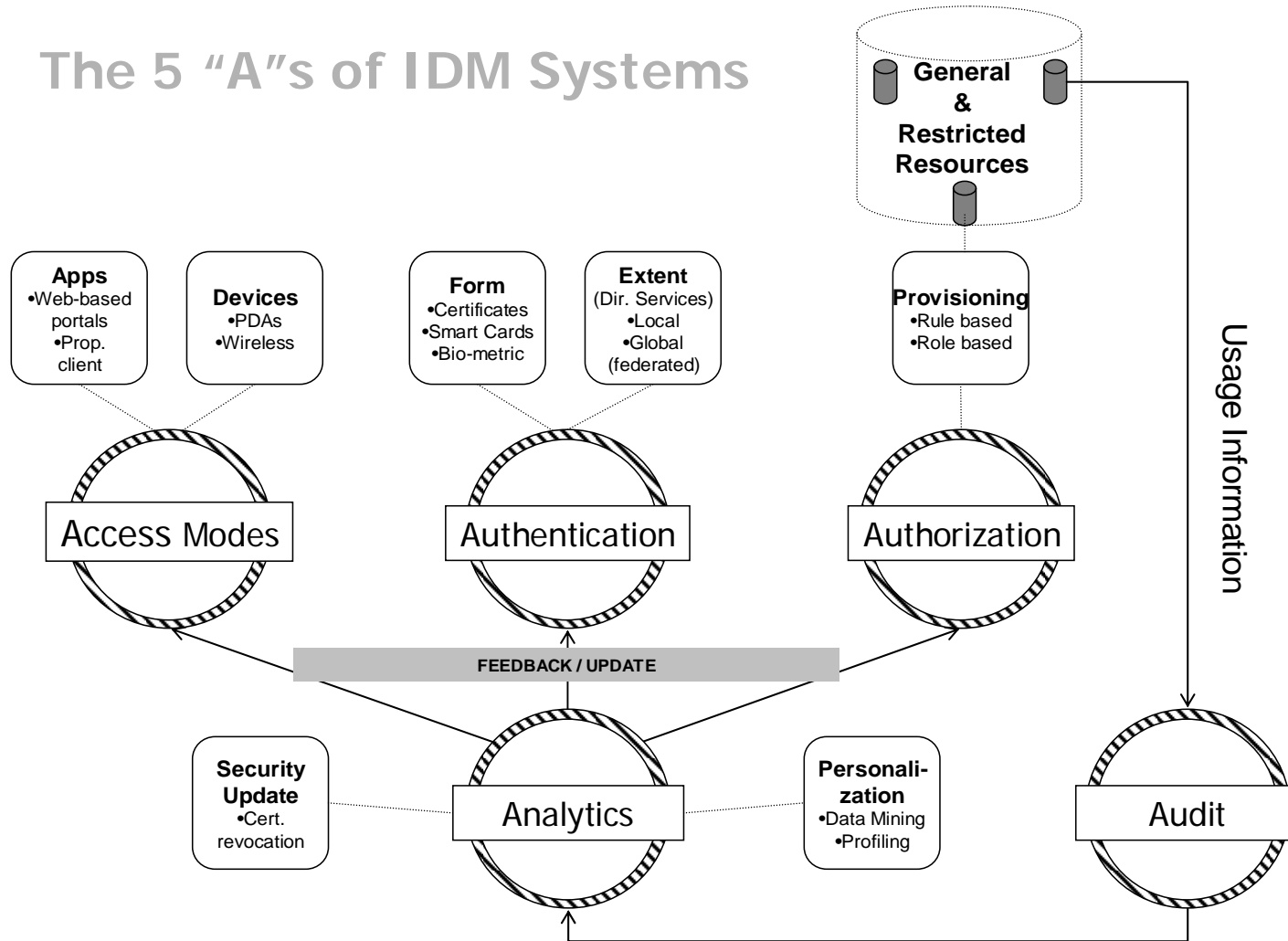
Technology Definition:

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

Technology Recommendations:

- 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.
- 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.

The 5 "A"s of IDM Systems



The Nodes: Process

Process Definition:

- 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

Process Recommendations:

- Information Security Risk Assessment
- Information Security Strategy
- Security Controls Implementation
- Security Testing
- Monitoring and Updating
- Level 4 Commitment Focus
- Level 5 Systemic

The Tensions: Human Factors

Human Factors Definition:

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

--Majchrzak

Human Factors Recommendations:

- Take steps to close the gap between technology and people so that they can co-exist and create a synergistic environment.
- Provide additional training, documentation, and in some cases user-friendly interface custom applications.
- Take further steps by spreading security awareness and knowledge from a select group of IT staff to larger portions of their staff. (McCarthy)
- 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 (Majchrzak)

The Tensions: Culture

Culture Definition:

- The covert, *underlying* patterns of behavior, belief, assumptions, attitudes
- Emergent, learned, and often creating a sense of superiority and comfort.
- Passed to succeeding populations who tend to make the same assumptions of superiority, predictability, and comfort.
- Much stronger than just the additive effect of the people and organization nodes
- The DNA: How “stuff” really gets done in

USC organizations. (Kiely, 2001)

Culture Recommendations:

- **Develop “Intentional Cultures”** (Kiely, 2006)
- Provide knowledge, skills, and understanding of outcomes and rewards
- Develop consistency of processes and protocols for information sharing and protection such as Six Sigma (or simpler variations) that people trust
- Train then hold people accountable for these protocols
- Give people disciplined “voice” such as corporate dialogue programs
- Create behavioral standards (both in reward and consequence) regarding how mistakes and breaches are handled
- Develop scenario training to change beliefs and attitudes
- Develop internal oversight groups

The Tensions: Governance

Governance Definition:

The Board and the C-suite executives:

- Align actions of organization's individual parts toward aggregate, mutual benefit
- Provide means for individual parts of the organization to trust other units to make contributions toward mutual benefit
- Provide means for information to quickly flow among various stakeholders
- Ensure that changing nature of stakeholder needs/desires and environment get effectively factored into decision processes
- Ensure the conditions for directors and managers to act in the interests of the firm, its shareholders, and its workers
- Ensure the means to hold leadership accountable to investors and employees for the use of assets

Governance Recommendations:

- Understand the criticality of security issues
- A different attitude regarding governance role and duties
- Emergent, cross-industry communities of interest and communities of practice who could develop standards
- New security knowledge and criteria for CEO selection, performance review, and compensation
- Require development and education for Boards and C-Suite as part of new self-regulating standards
- Criteria implemented corporation-by-corporation
- Hold vendors and suppliers accountable for implementing these standards/criteria

Other Requirements of the Board:

- Clear understanding of assets, risk, and mechanisms to protect the enterprise.
- **Clarity regarding the relationship between board and management in security responsibilities**
- Redefinition of the “Duty of Care” responsibilities to include knowledge and prudence regarding issues of potential harm or potential crises
- Redefinition of the “Duty of Supervision” responsibilities to include knowledge and prudence regarding issues of potential harm or crises as criteria for choosing and placement of executives
- Threat assessment audits similar to current fiscal audit committees with neutral auditors
- Comfort on the part of the board that management has ability to make decisions regarding prevention and protection of the enterprise

New CSO or CPO positions

The Tensions: Architecture

Architecture Definition:

- Architecture 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

Architecture Recommendations:

- The DoDAF defines architecture in terms of three related views:
 - Operational View
 - Systems View
 - Technical Standards View (2003)
- 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 Tensions: Enabling and Support

Enabling and Support Definition:

- 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, 2001)

Enabling and Support Recommendations:

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. (El Sawy, 2001)

The Tensions: Emergence

Emergence Definition:

- Inherently “not routine”
- Not amenable to a top down approach
- Interactions of each part of a system and its immediate surroundings cause a “complexity which leads to order”
- Outcomes are not predictable
- More than the sum of the parts
- Emergent order will not arise if are simply coexisting; the interaction of the parts is central
- The new, the unpredictable, the emergent is a part of every organization
- A major security concern and a potential place for solutions to occur.

Emergence Recommendations:

1. **Build a Thinking Organization** (Kiely, 2002)
2. Build in process rigor, feedback loops, critical thinking, and creativity into daily practices
3. Use rigorous processes and innovative practices in assessing potential liabilities and risks.
4. Align with "Process" node by ensuring the emergent nature of process improvement
5. Align with "People" node by creating new cultural norms and DNA
6. Develop groups and individuals who are specifically focused on possible sources and means of harm
7. Ensure behaviors are demonstrated consistently by C-Suite and boards
8. Build the above into all decisions, projects, etc.
9. Expect and embrace radical emergence, not just the incremental emergence of continuous improvement.
10. Establish governance policies that support and reinforce the above both in attention and budget

Conclusion

1. Understand interconnectedness in the ICIP model
2. Put protection and preservation at the same level as progress and profit
3. Build protection and preservation behaviors into the design and strategy of the organization
4. Create a new focus on security issues in recruiting, placing, and managing personnel
5. Increase the emphasis on information security technology and identity management

6. Include protection and preservation of the organization in all formal processes
7. Pay close attention to the human factors that are caused by the interaction of people and their actual use of technology
8. Know that most of the problems and solutions for security issues lie deep in the DNA or cultural level of an organization
9. House responsibility for security of all tangible and intangible assets with the Board and the C-suite executives
10. Architect the technology and its use to be aligned with organization's design and strategy: protection and preservation as well as progress

11. Create and develop 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. Use emergent methods to ensure not only “learning” organizations but more importantly “thinking” organizations.
13. Recognize that this is a dynamic process not a linear model demanding that we constantly circle back to balance the tensions and maintain eternal vigilance

Finally

Acknowledge that this boat has sailed and we're either on it or we're waving goodbye

