



intralot

Managing Information Security in the Dynamic Corporate Environment

Dr. Christos K. Dimitriadis
Security Officer
INTRALOT S.A.



intralot



Agenda:

- **Characteristics of the modern corporation.**
- **Facts and Open Issues in Information Security Management.**
- **Systemic Thinking towards complex Problem Solving.**
- **A novel business model for information security management.**
- **Case study.**
- **Conclusions.**

The modern Corporation

- Operate in a non-static global business environment that requires dynamic plan execution:
 - Strategic Function: Definition of goals.
 - Operational Function: Paths to achieve goals.
 - Human resources function: Organizational structures – roles.
- The three primary business functions are dynamic themselves for addressing the dynamic business environment.
- Information Security must be an integral part of the business.
- Are static Information Security Models sufficient?

- Information has many forms: electronic, paper, oral.
- Information has complex flows within and outside the corporation.
- Information protection problems are complex and involve multiple parties.
- Globalization introduces diverse cultures, behaviors, beliefs within a multiethnic environment.
- External influences cause operational processes to change creating a sense of uncertainty in information security.

- Many problems appear not to have been solved regardless of past actions taken.
- Isolated cause and effect thinking for problem solving is not effective.
- Continuous fire fighting mode results in little time for innovation.
- Over-reliance on technology is not sufficient to solve problems.

- Why?
 - Are all variables in the business environment considered?
 - Are these variables correlated in order to address security as a whole?
 - Is the human factor given the appropriate attention?
 - Are existing ways of dealing with issues working for all parties?

Adopting systemic thinking

- Systemic thinking is relational. Relationships between actors are crucial.
- View towards the interaction among components of systems rather than individuals.
- Organization resources combine and interact in an order intrinsic to the purpose and objectives to be delivered and must be managed as such.
- The systemic view is orientated towards the long term.
- Systems tend to preserve themselves so actors tend to become accustomed to habits.

A Dynamic Information Security Model

Developed by ISACA SMC/BMD committee to address the complexity of security, addressing security in a holistic and dynamic manner.

Elements

- Organization Design and Strategy
- People
- Process
- Technology

Dynamic Interconnections

- Culture
- Architecture
- Governing
- Emergence
- Enabling and Support
- Human Factors

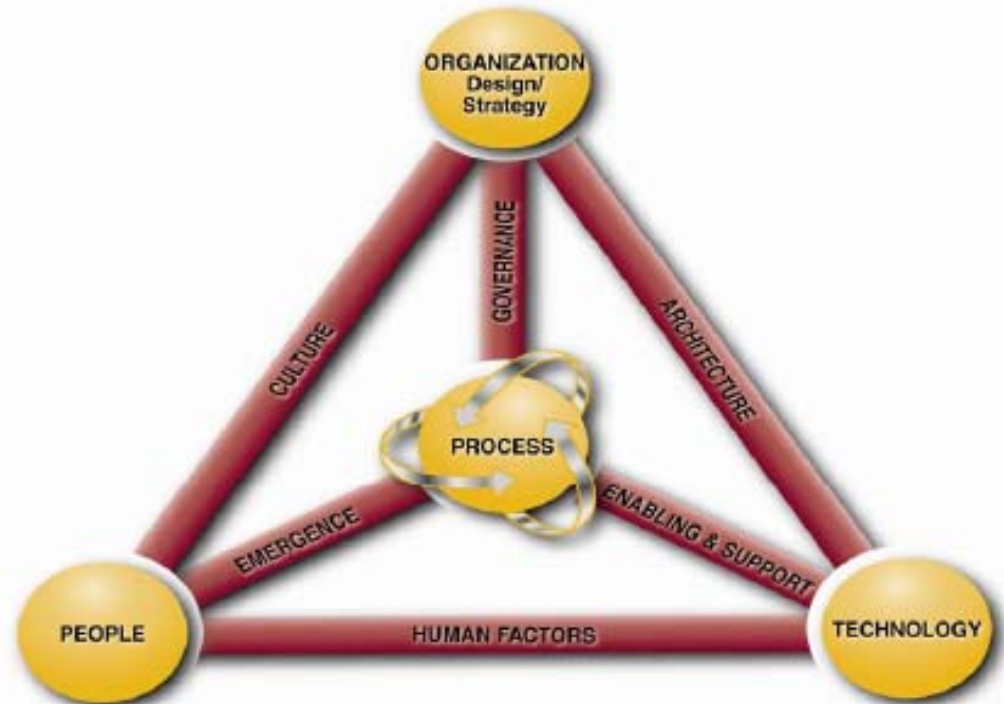


A Dynamic Information Security Model

Can be viewed as a three dimensional fluid model.

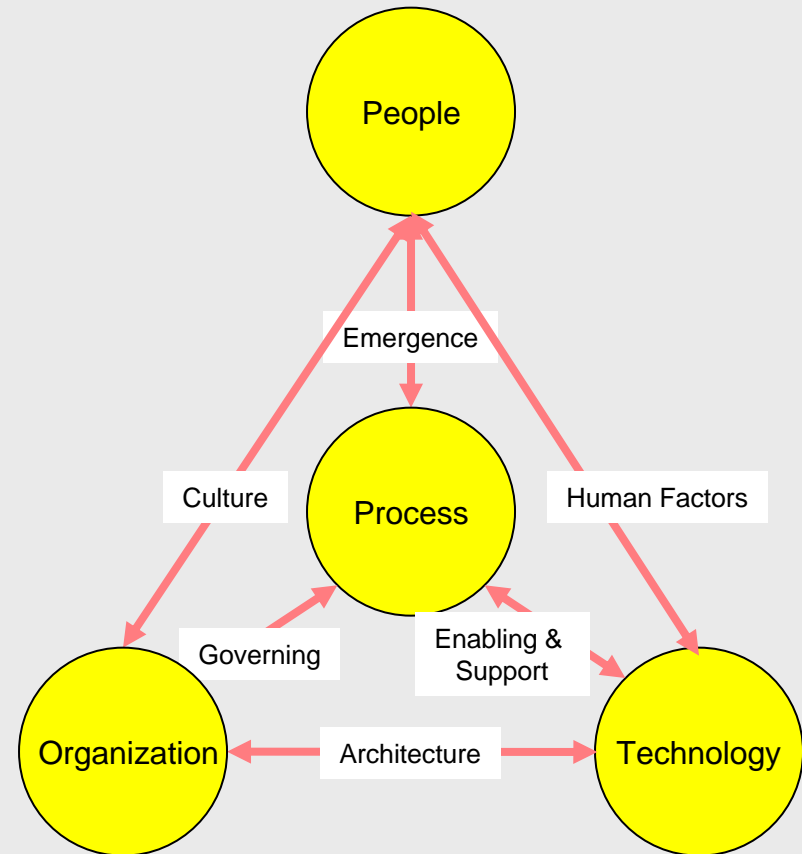
All aspects of the model interact with each other.

If any one part of the model is changed, not addressed, or managed inappropriately, it could distort the balance of the model.



Focus on People

- Represents the human resources and the security issues that surround them
- Collective of human actors including values and behaviors
- All whose efforts must be coordinated to accomplish the goals of the organization
- Not just units of “one” since each individual comes with all their experiences, values

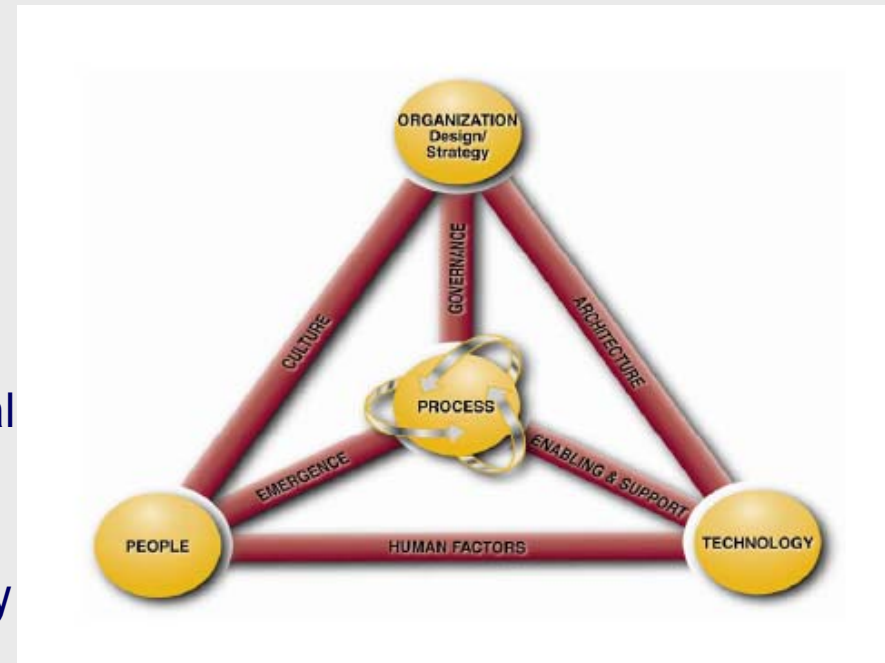


INTRALOT S.A.:

- **Multinational presence: More than 40 installations in five continents.**
- **Intensive security needs due to its operation in the Lottery Sector.**
- **Strategic direction for dedication to Research and Development projects for maintaining leadership in innovative technology.**
- **ISO 27001 / WLA SCS 2006 Certified.**

Case Study

- Culture: different cultures, behaviors, beliefs, ways of doing business.
- Human Factors: different reactions to security technologies.
- Emergence: customized procedures according to user acceptance.
- Governing: diverse managerial structures and strategies for managing each subsidiary.
- Architecture: different security needs require different information security strategies.
- Enabling and Support: customized combination of technologies and processes.



- Create a better understanding of the big picture.
- Obtain the greatest benefit from innovation efforts.
- Make innovation more strategically useful and beneficial.
- See the element (security) as part of the big picture.
- Understand the feedback relationship between what is studied and other parts of the system.
- Envision different environments so that change becomes indispensable.

Thank you

*Dr. Christos K. Dimitriadis, CISM, CISA
Security Officer*

intralot

[W] www.intralot.com

[e-mail] dimitriadis@intralot.com

intralot