



Rethinking Information Security Management

The Business Model for Information Security





What's wrong
with this
picture?





Traditional view of security



- Identify sensitive information
- Identify where it is located
- Create a boundary between inside and outside
- Trust everything inside
- Don't trust anything outside
- Monitor attempts to breach the fortress walls
- Measure security performance by cost of incidents
- Get recognized by selling **FUD**



Why we need to think differently

- Information cannot be contained
- There is no inside or outside
- Business value is driven by the ability to use information
- Budgets are not determined by how much an incident costs
- The “C” suite does not really understand information security
- Techno babble is not spoken at board meetings

**NOW
OPEN**



Critical Elements of Information Security Program Success

*In each group identify 5 things that **most** impede information security program success.*



Most significant challenges confronting information security managers

- Senior Management commitment to information security initiatives
- Management understanding of information security issues
- Information security planning prior to implementation of new technologies
- Integration between business and information security
- Alignment of information security with the organization's objectives
- Executive and line management ownership and accountability for implementing, monitoring, and reporting on information security

Source: Critical Elements of Information Security Program Success, ISACA, 2005



Security Often Laments

IF Only.....

- I had better tools
- Users understood security
- I had enough resources
- Security was a top priority
- We had stronger regulations
- People read and understood security policies





THE TRUTH IS

- Technology will never be able to solve our information security problems
- Security awareness programs do not change behavior
- Point solutions only solve point problems.
- More effort will not provide better results
- Quick solutions quickly come back as even more difficult problems



WE NEED AN APPROACH THAT...

- Help us to envision solutions to problems
- Communicates in business language
- Aligns information security and organization goals and strategies
- Makes the best use of available resources
- Focuses on business risk
- Contributes to value creation



PROBLEM STATEMENT

Current models for information security do not adequately represent what the components of an information security program are or how an information security program functions.



A MODEL IS

- Representation of something
- A representative form, style or pattern
- A simplified representation or description of a system or complex entity, esp one designed to facilitate calculations and predictions
- A systematic description of an object or phenomenon that shares important characteristics
- A description of a complex entity or process

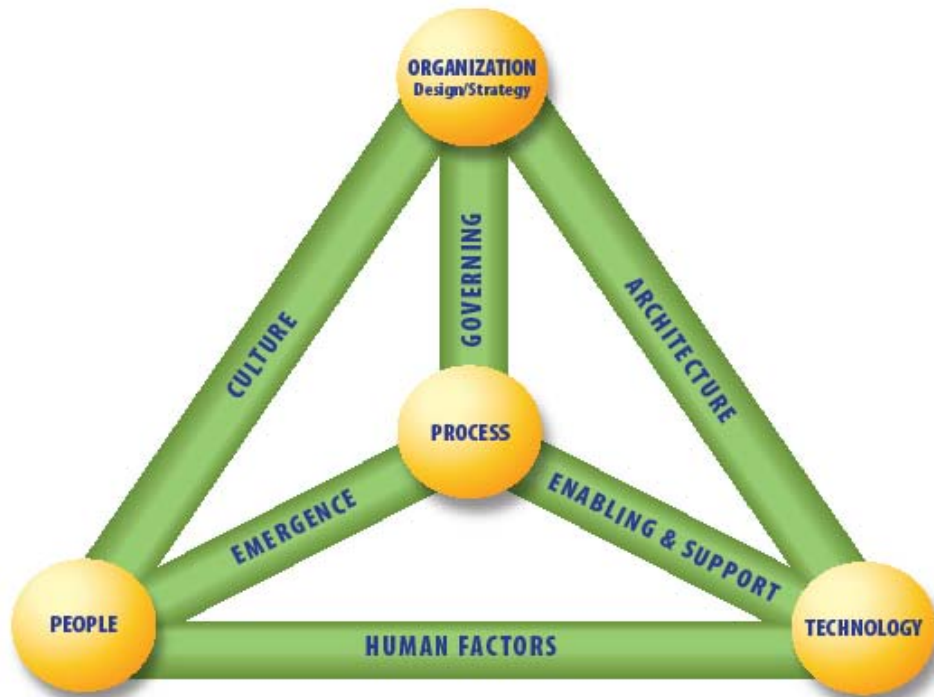




A SECURITY MODEL CAN TEACH US

- How to look at a problem – to determine causes rather than symptoms
- How to use resources for maximum impact – less often provides more
- How components interact and influence
- How to identify and use leverage points

BUSINESS MODEL FOR INFORMATION SECURITY



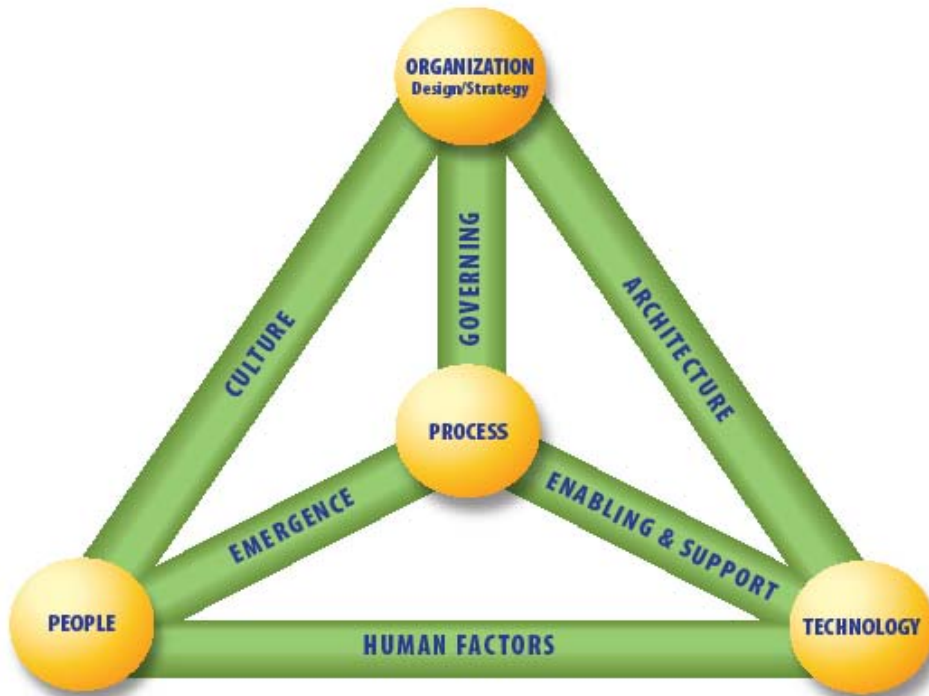
Business orientated model conceived by the University of Southern California Marshall School of Business to address the complex challenges of protection.

Developed by ISACA to provide a practical approach to information security management comprehensible and useable by business and security practitioners.



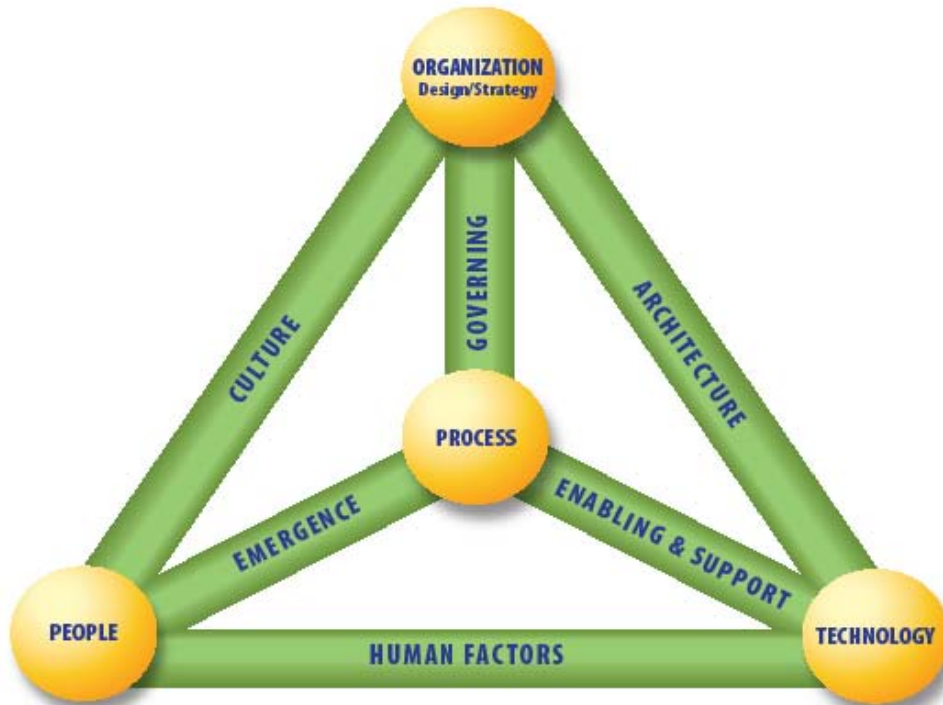
Holistic Approach

Emphasizing the importance of the whole and the interdependence of its parts





Systemic Thinking



Relating to or affecting the entire body or an entire organism

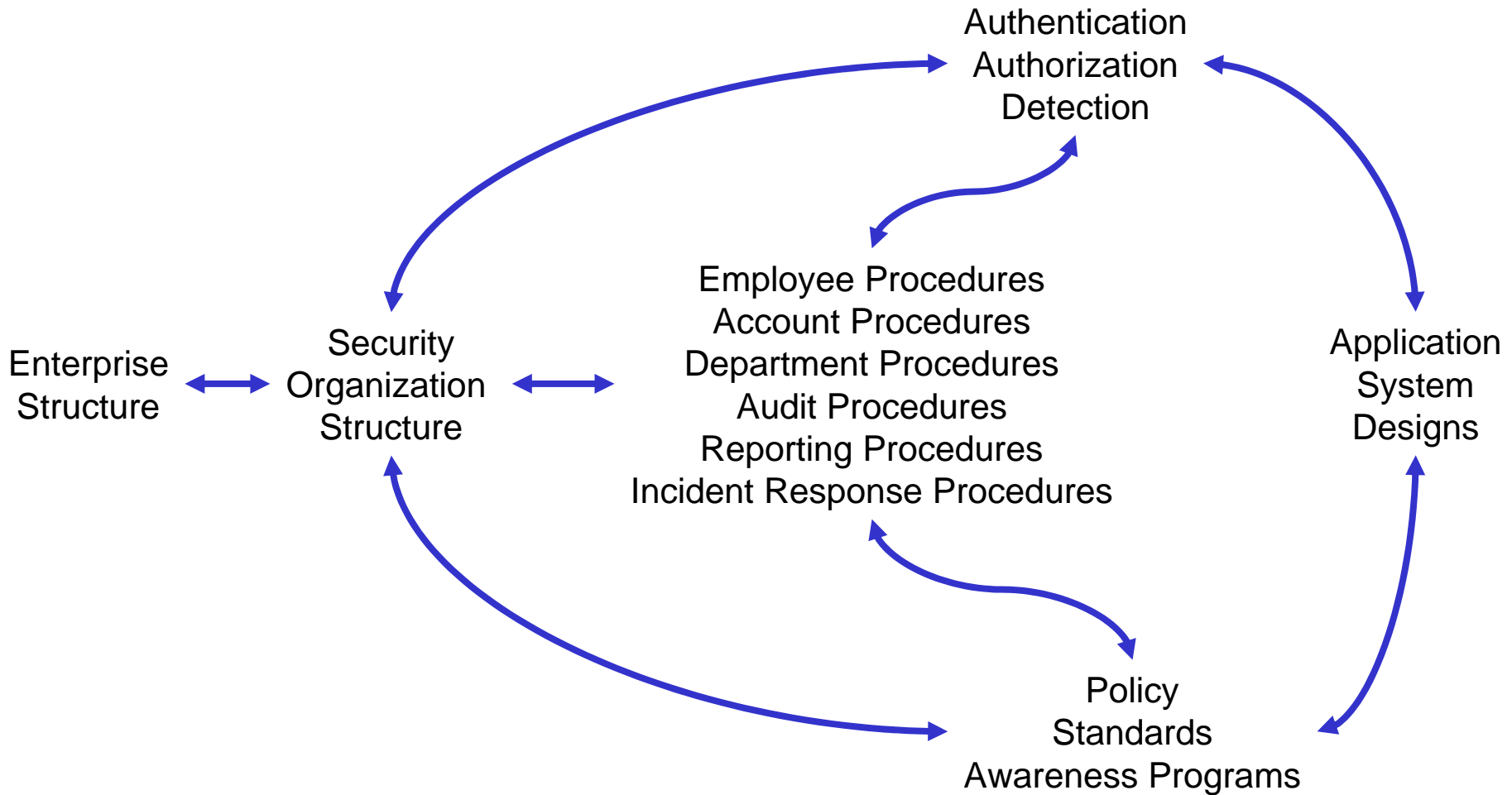


Anatomy of a Systemic Security Problem





COMPONENTS OF A SECURITY SYSTEM





ANATOMY OF A FRAUD

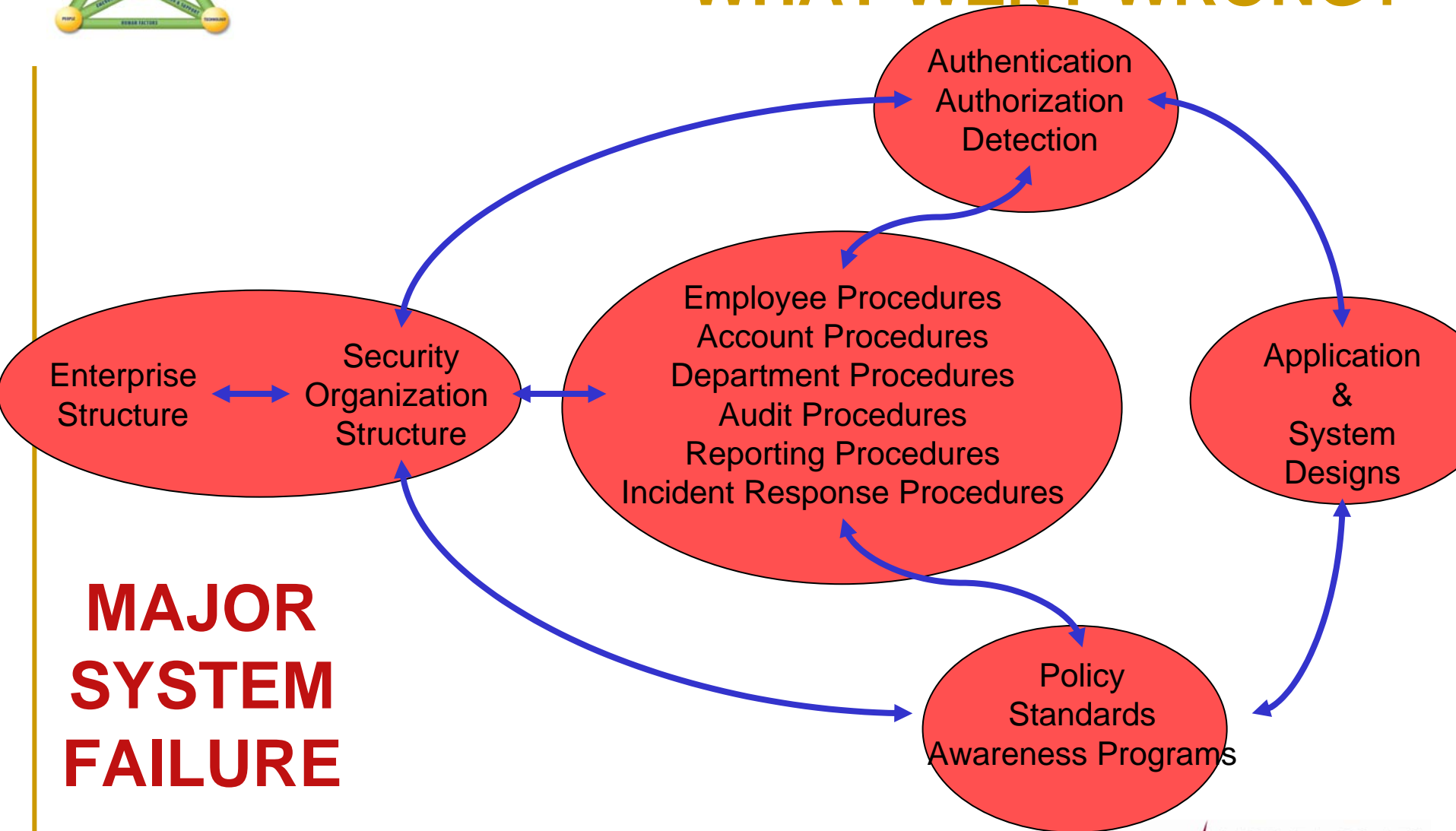
Rogue trader causes \$7 billion loss - unauthorized transactions

- Compromise of system accounts
- Lack of investigative follow up
- Poor management supervision
- Spoofed activity
- Inadequate application controls
- Awareness used for malicious activities
- Misaligned corporate culture





WHAT WENT WRONG?



**MAJOR
SYSTEM
FAILURE**



Recommended Solution

- Biometric Authentication
- Improved Alert Procedures
- Tighten Trading Controls



MOST SIGNIFICANT ISSUES

System Imbalance – you can do the right things and still get the wrong results

- Reliance on technology to control access
- Reliance on procedures to control behavior
- Reliance on awareness to shape behavior
- Reliance on management to monitor performance
- Reliance on multiple system components to perform in harmony

Culture Failure

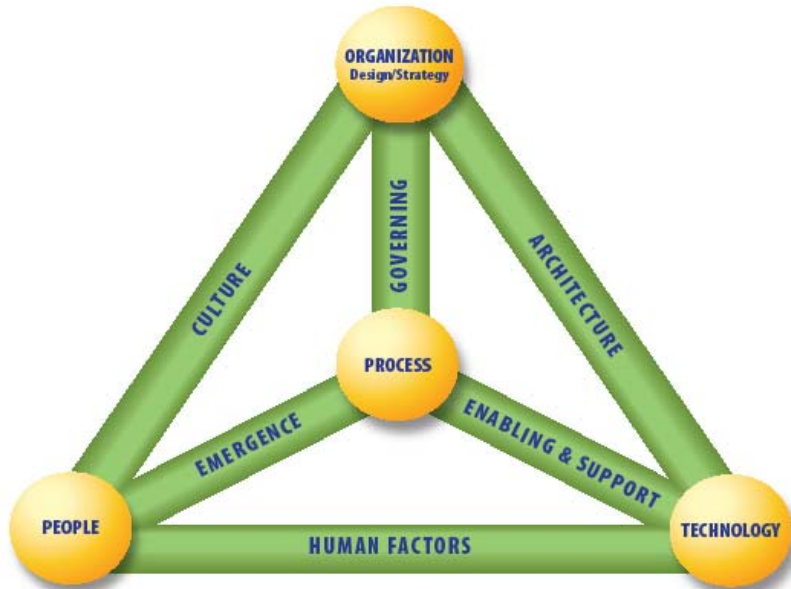
Culture is a shared, learned, symbolic system of values, beliefs and attitudes that shape and influence perception and behavior
(<http://www2.eou.edu/~kdahl/cultdef.html>)



The Business Model for Information Security



CORE CONCEPTS



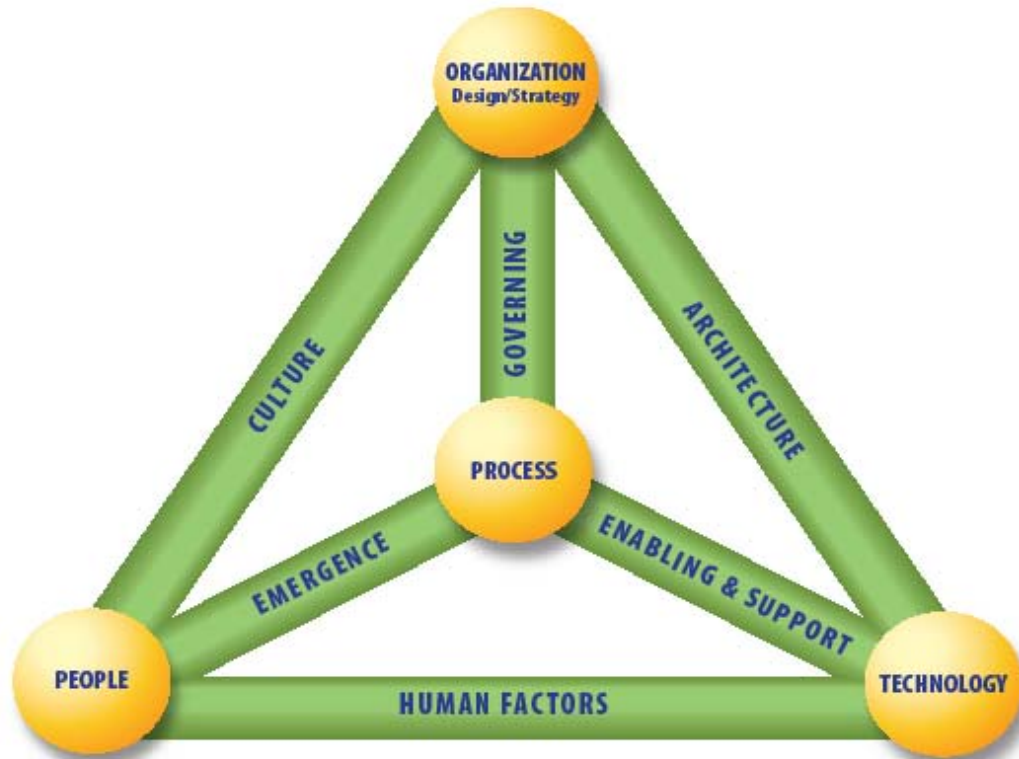
To improve performance you have to change the system.

To change the system you have to change the way you think.

- People, process, technology and organization are neither bad nor good
- Culture, architecture, human factors etc influence the elements of a security system to produce or inhibit risk
- Look for leverage points in designing security system

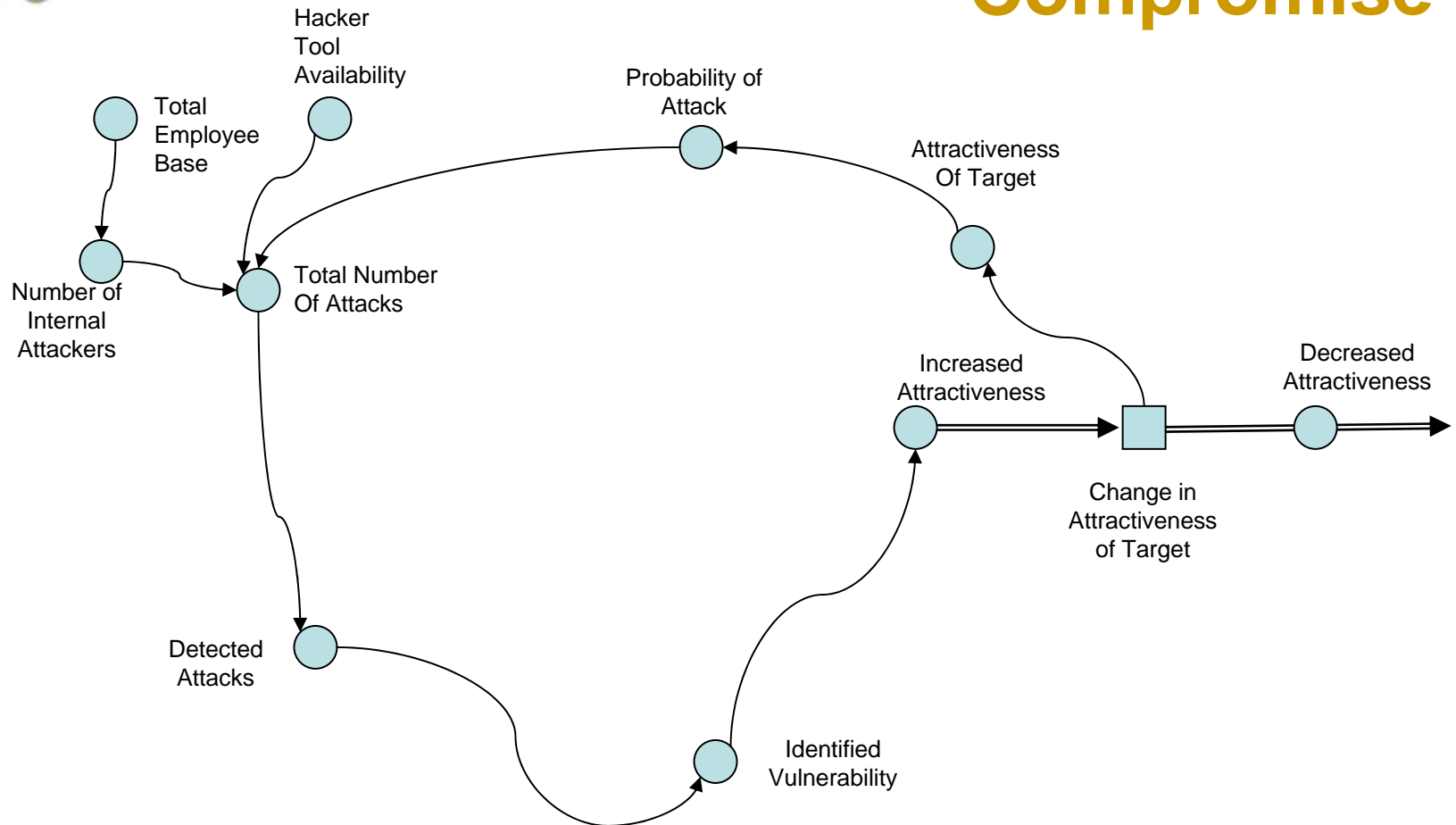


How the Model works



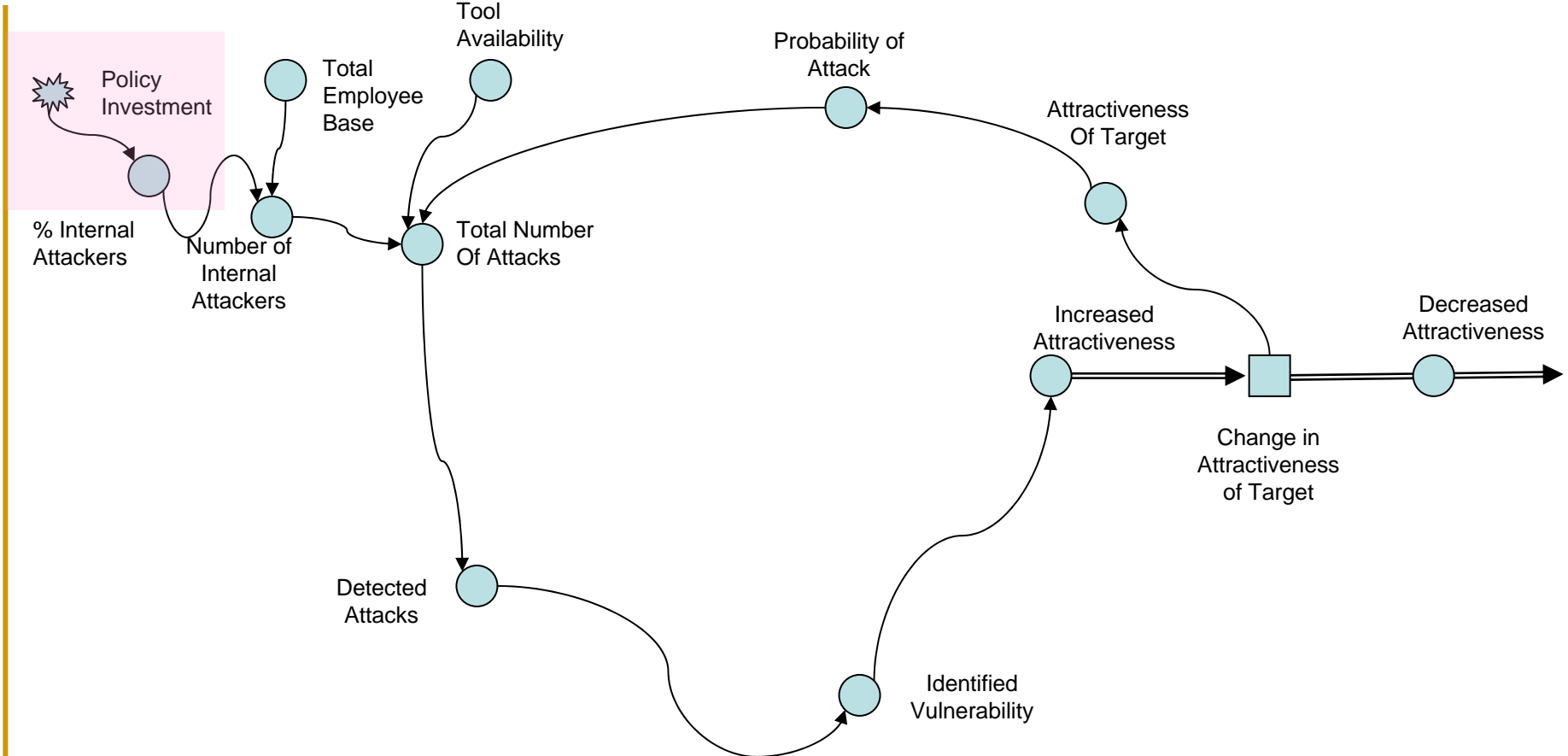


System Dynamics Model – Internal Compromise

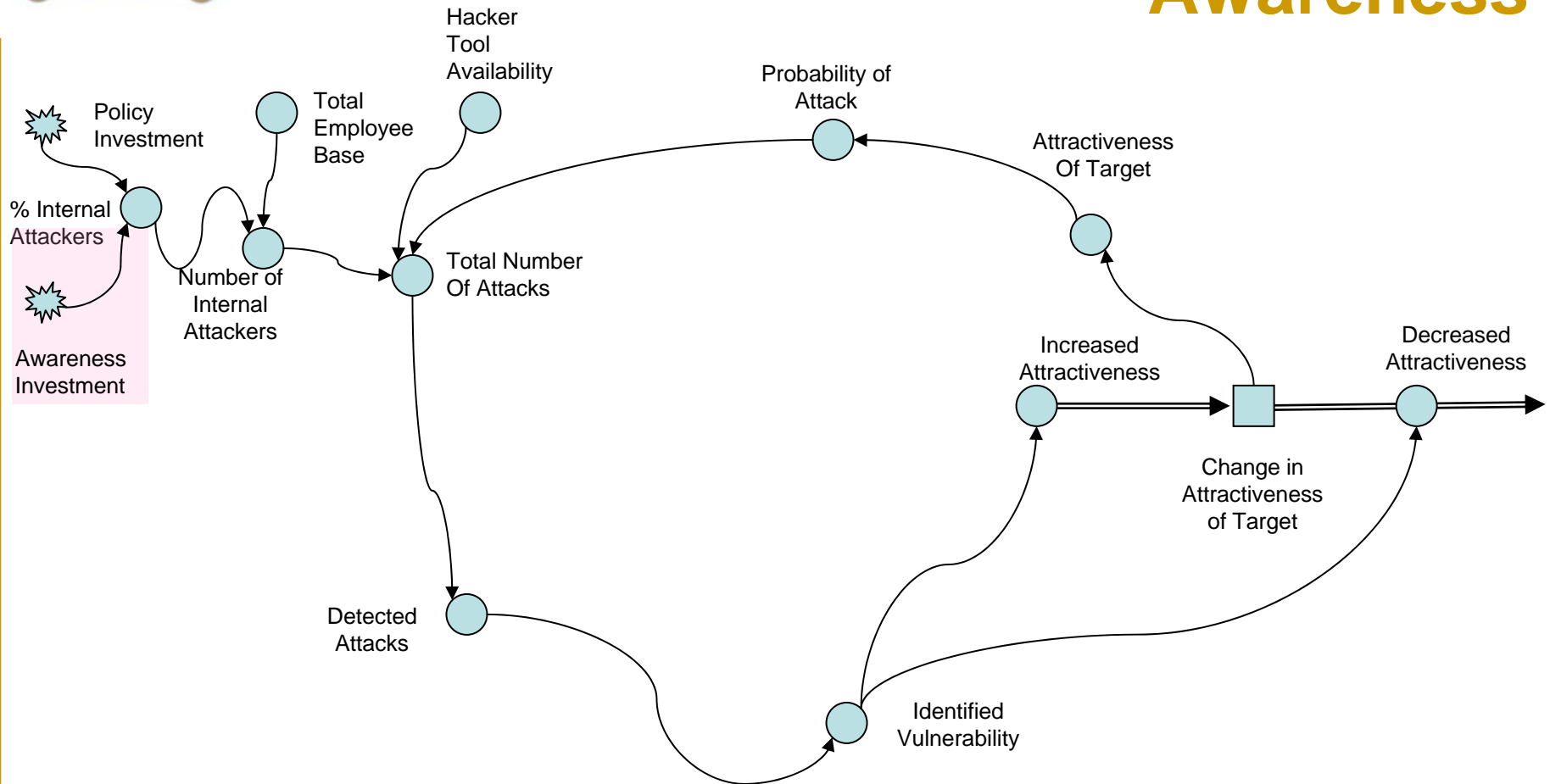




Internal Compromise - Add Security Policy

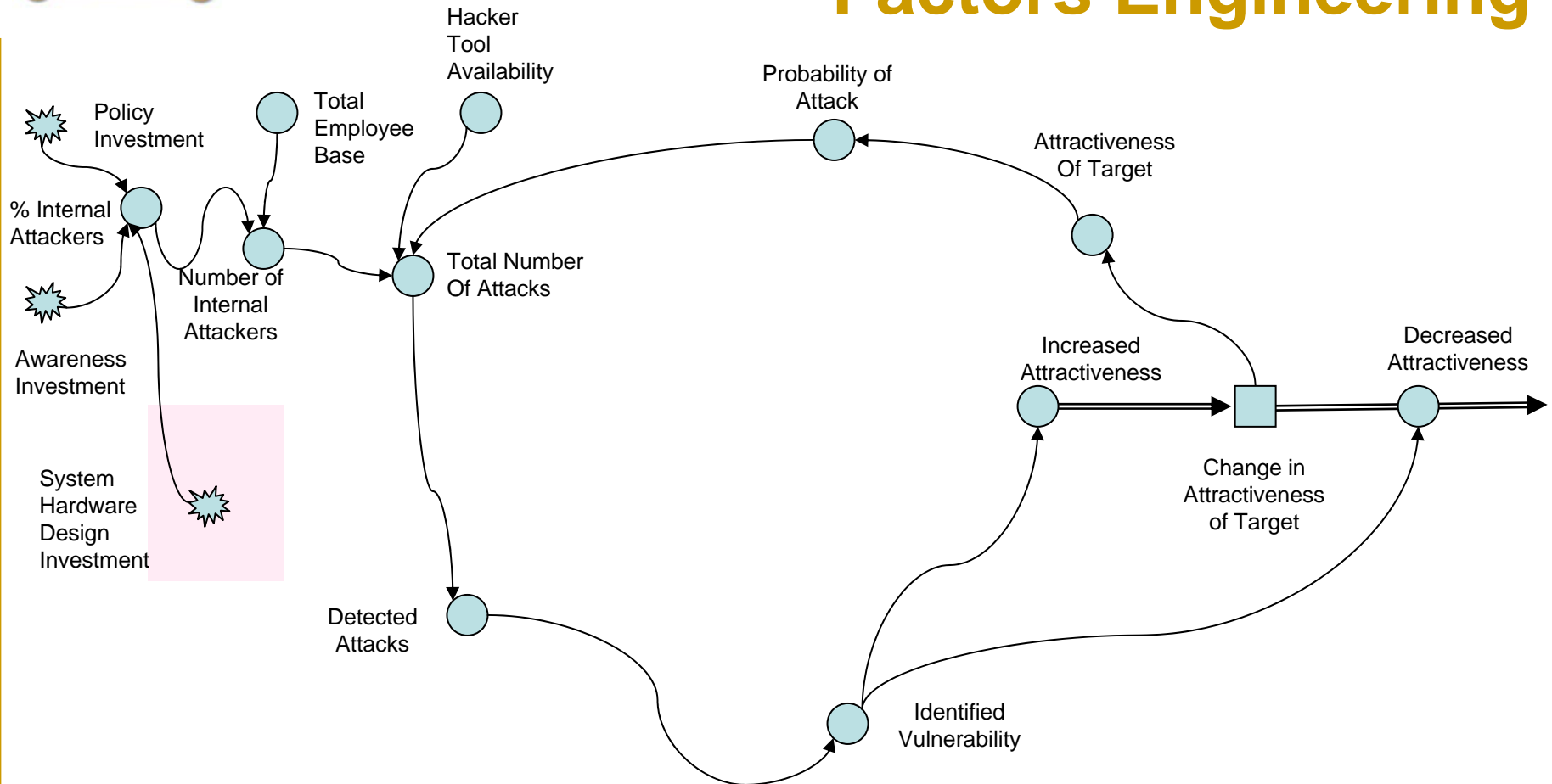


Internal Compromise – Add Awareness



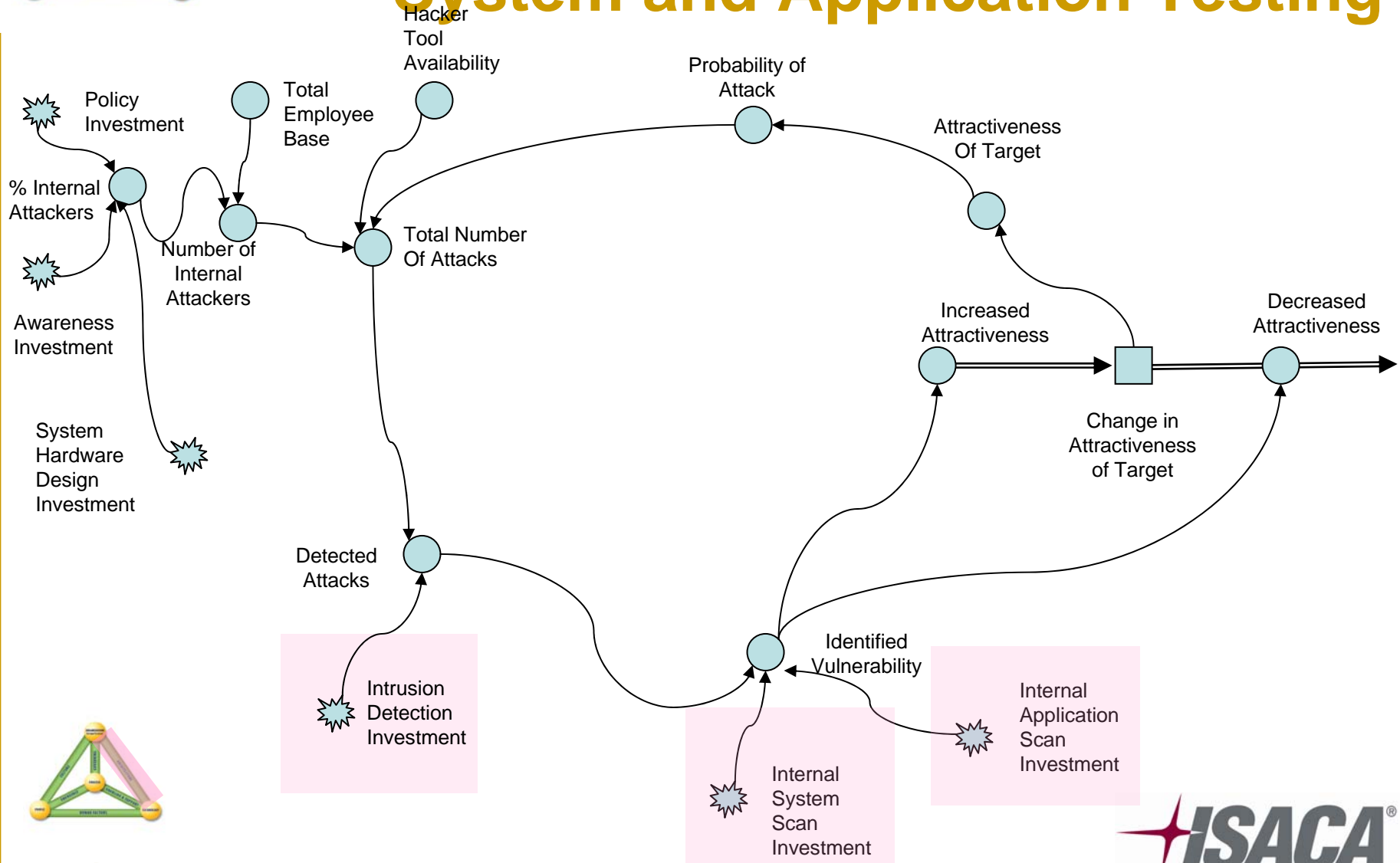


Internal Compromise – Add Human Factors Engineering

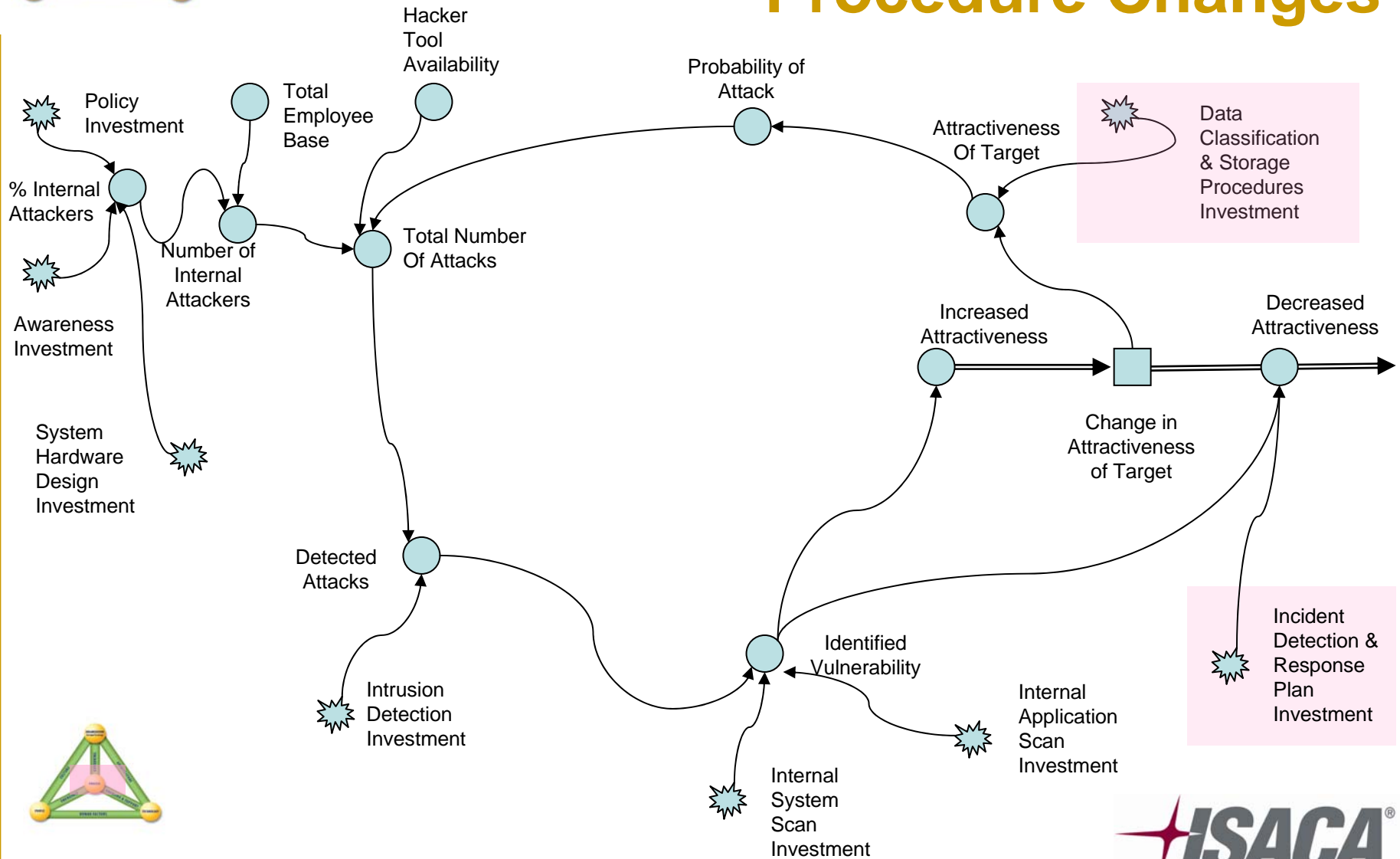




Internal Compromise – Add Internal System and Application Testing

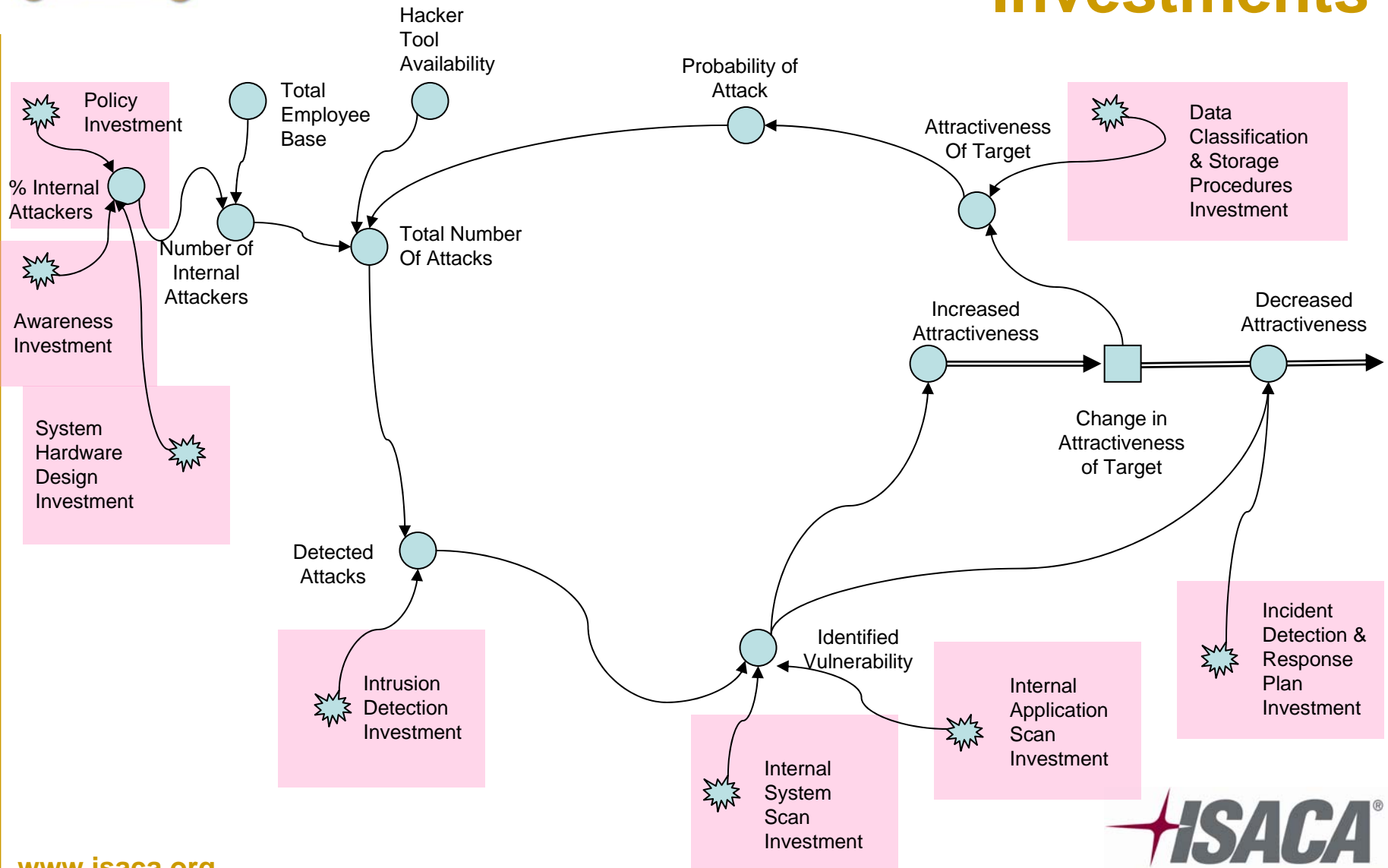


Internal Compromise – Add Procedure Changes





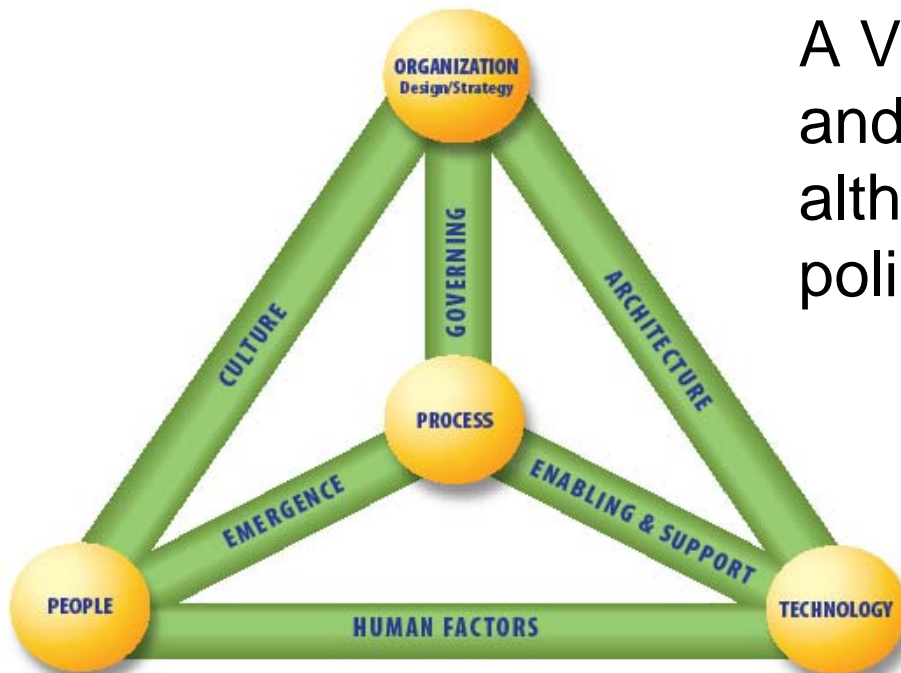
Systems View of Security Investments





Considering Some Situations

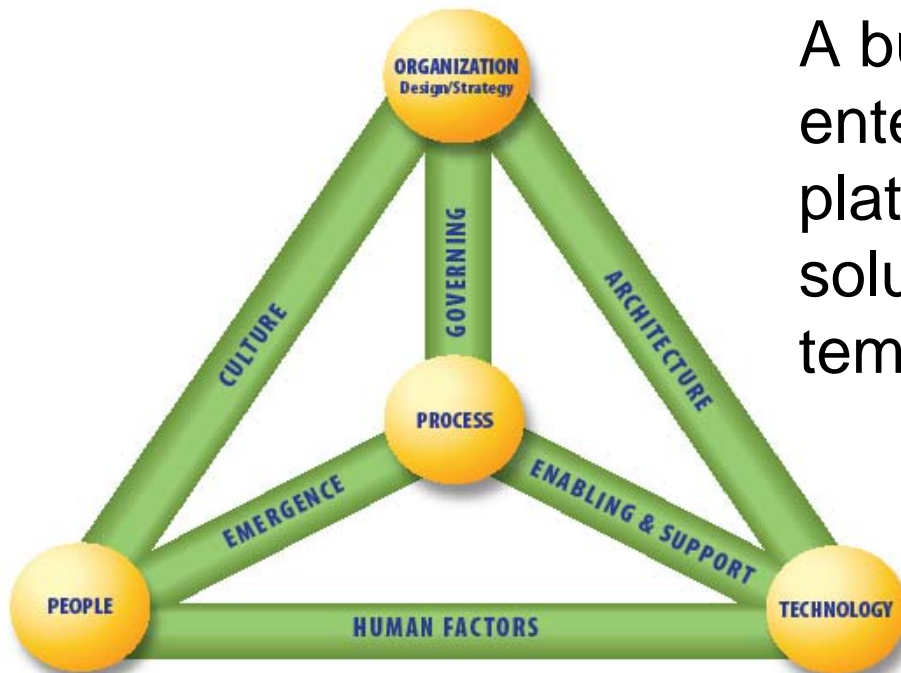
A VP purchases a new iPad and begins using it at work although it is clearly against policy





Considering Some Situations

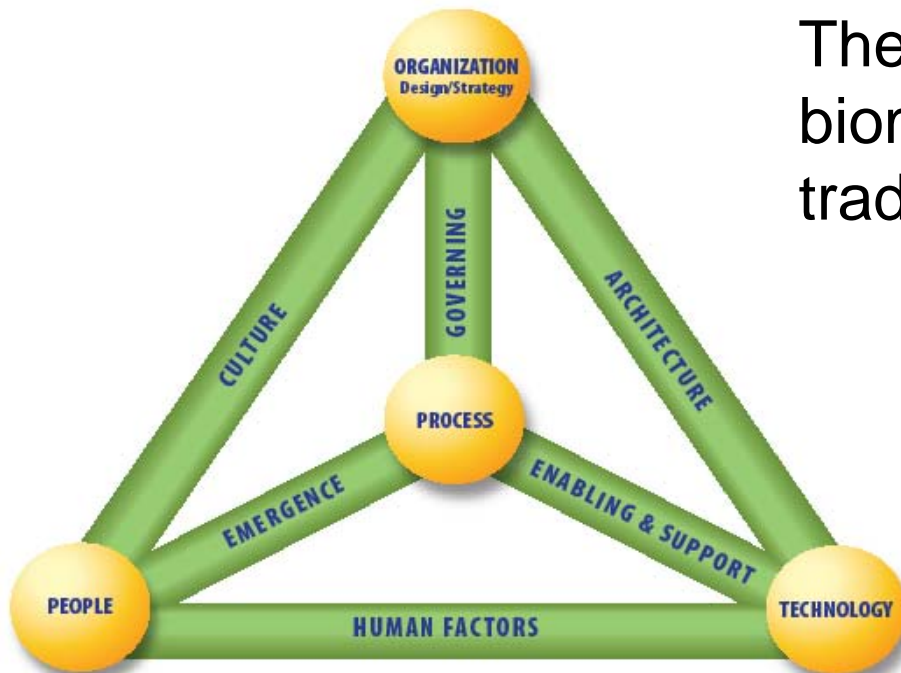
A business unit manager enters into a contact for a platform as a service cloud solution to support a temporary department need.





Considering Some Situations

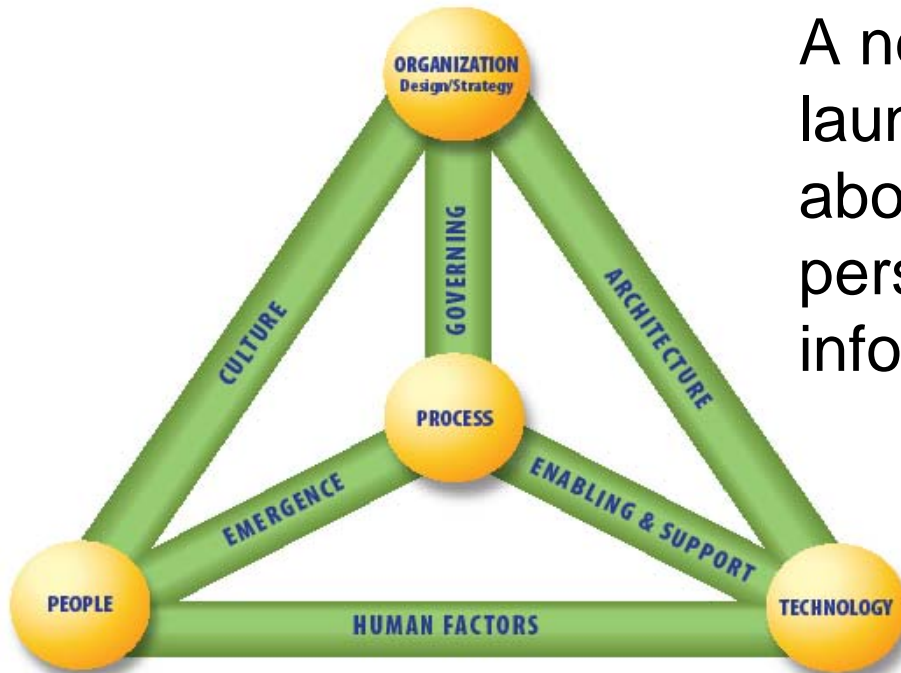
The bank implements biometric authentication for trading systems.





Considering Some Solutions

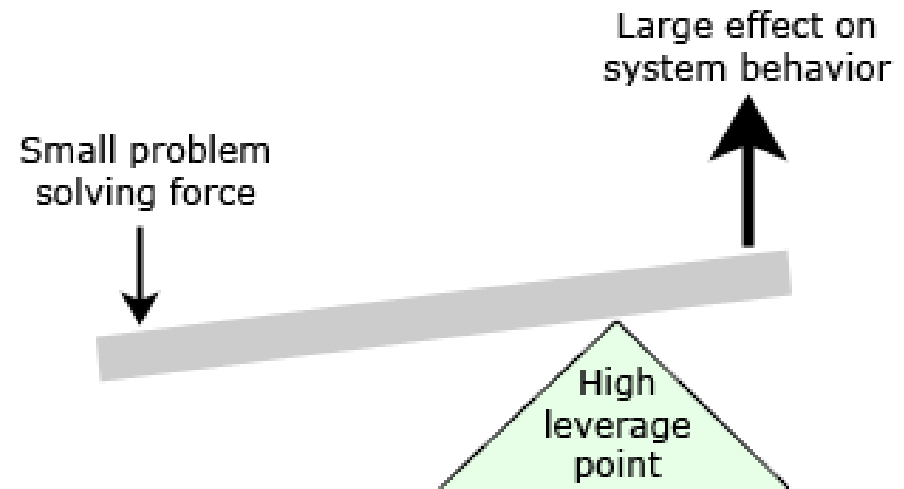
A new awareness program is launched to inform workers about the need to protect personally identifiable information.





LOOK FOR LEVERAGE POINTS

A **leverage point** is a place in a system where force can be applied. A **low leverage point** is a place in a system where a small amount of force causes a small change to system behavior. A **high leverage point** is a place in a system where a small amount of change force (the effort required to prepare and make a change) causes a large amount of predictable, favorable response.





Example – Campus Security



Problem – need to provide quick notification of campus security incidents to all staff, faculty and students.

Solution – use IM to notify students of incidents on campus and surrounding areas.

Result – greater sense of personal safety
Ability to quickly secure an area
Enhanced reporting and notification



Example – Employee Recognition Program



Problem – employees do not recognize their personal responsibility for protecting information.

Solution – recognize positive security behavior on a monthly basis by awarding a \$100 reward check for exemplary security behavior.

Result – Positive behavior is rewarded.



Example – Security Team Member



Problem – sales people had been outbid on projects and were concerned that sensitive proposal information had been compromised.

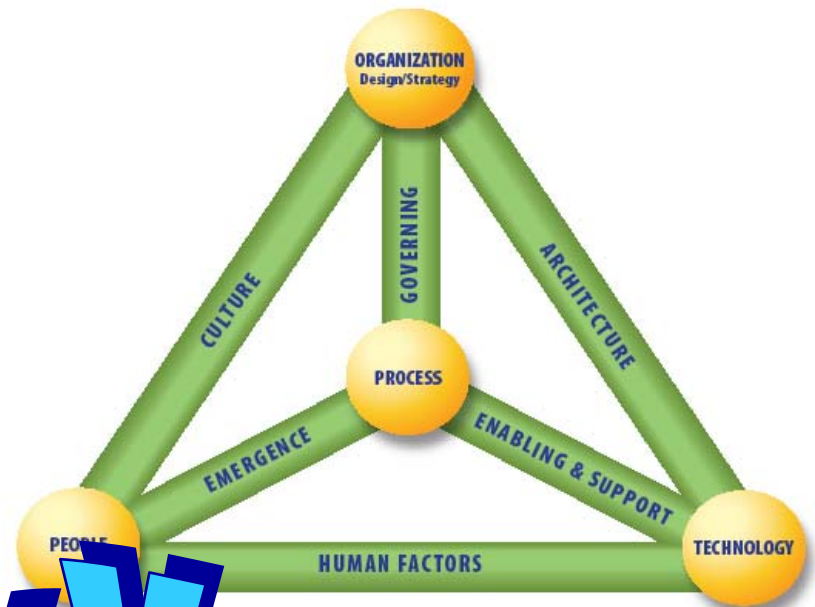
Solution – a security representative was assigned to sales and worked as part of their team to help understand sales challenges and security threats. Security established a site where current threat levels could be posted. It also provided information about potential for espionage and theft of sensitive business information.

Result – Security was seen as an enabler supporting sales people in the field to do their jobs better.



TAKE AWAY

- What we do in security is not wrong
- How we think about security can be improved
- How we deliver solutions can benefit from a holistic systems approach
- Remember that customers want solutions that respond to their needs



Thank You