



---

# Information Security and Privacy as a Service: solving\* intractable problems

1 October 2009





# Agenda

---

## What we'll cover today

- Introduction
- Platonic Ideals vs. Tough Situations
- Planning
- Implementation Strategies
- Discussion & Questions



## Jon Espenschied

- Director, Information Security Consulting
- 20+ years in IT, security & privacy, with the usual acronym salad: CISSP, CISA, CISM, CGEIT, former QSA/QDSP, MSRA, IAM, GIAC/GISO, etc
- Formerly with UN, Symantec, @stake, CTG, Sierra Systems, AT&T Wireless, Microsoft

## Consciere LLC

Information security consulting, from governance & strategy to technical assessment and pen-testing

Seattle, Denver, Chicago, San Francisco



## Ideals vs. Tough Situations



# Ideals vs. Tough Situations

---

## Platonic Ideals

- Governance & Program are defined
- Security Authority
- Cooperative Business – wants assets secured
- Security Policies – Enterprise and Lower-Level
- Security Standards – often ISO 27002
- Security Procedures or Technology Controls
- Cooperative Operations



# Ideals vs. Tough Situations

---

## **Tough Situations:**

### **Ineffective or nonexistent security**

- No management authority
- Lack of governance
- Weak or nonexistent policies
- Nonstandard standards
- Procedures or configurations masquerading as policies



# Ideals vs. Tough Situations

---

## **Tough Situations: Causes are Plenty**

- Singular Focus
- Disorganization (not enough focus)
- Organic Dysfunction (don't care)
- Uninformed (never thought about it)
- Mistrust (not invented here)
- Previous Failures (tried that already)



## **How can we ensure failure of our information security program?**

- Make it ineffective
- Lose respect
- Really drive it into the ground
- Your experiences?



## Planning

- Where you stand
- What needs done
- Can you succeed?



## Stop and Think

- Don't do those bad things; Don't fixate either.
- Rapidly deteriorating conditions: *"The first thing you gotta \$@%# do, is do not move!"* -ICP
- Most problems come from too much doing and not enough thinking.
- Consider how the situation will progress
- Plan the "Way Forward"



## **Map the Way Forward**

- Use assessments or audit findings
- Identify internal expectations and tasks
- IT security versus Information Security
- Compare to norms for your size & industry

## **Roadmaps or Information Maps**

- Figure out dependencies
- Get a handle on the next 1-2 years, maybe more



## Recognize a Fait Accompli

- Sometimes understanding is enough.
- Poker rule: *In every game, there's a patsy. If you don't know who the patsy is, it's you.*
- Spaf's First Law: *If you have responsibility for security but have no authority to set rules or punish violators, your own role in the organization is to take the blame when something big goes wrong.*
- ...and the employment listings: *e.g. a Security Lead job that gets re-posted every 6-18 months*



## **This is not a movie**

- Sometimes the organization does not want succeed (read Edward Yourdon's "*Death March*")
- If you can't succeed, get out.
- Martyrdom is overrated.
- But..... There's always some wiggle room. You may still take on a death march for experience or affiliation



## Implementation Strategies

- Direct Approach
- Methodical
- Service Approach
- Political



## Direct Approach

- *If this works, you don't need me.*
- Clearly state information security & privacy need
- Propose a security program, policies, and controls
- Get management and executive buy-in
- Consists largely of notifying responsible leaders (not "Managing Up" or other nonsense that's good for your career, but not the organization)



## Methodical Approaches

- Consists of convincing reasonable leaders.
- Identify assets, conduct a risk analysis.
- Benchmarks – *"we're the only one NOT doing X" is often very compelling to legal and execs.*
- Assemble or adopt components of authority (LOB, legal, finance, HR)
- Define top-down program components.
- Define a policy & standards process, form committee, and start work tasks.



## **Service Approach – Viable as Bottom-Up**

- Identify assets, conduct a risk analysis
- Integrate with IT services
- Offer security as a feature of net/OS/app
- Security becomes a part of proper operations
- Build standards from proven operations
- Draft policies to support accepted standards



## **Service Approach – Planning Ahead**

- Mapping: identify a customer for every task
- Every security directive has a business driver
- Every security standard is presented as proper operation of IT services (performance standards)
- Security controls presented as satisfying requirements for integrity, access, confidentiality
- Communicate constantly



## Service Approach - Case Study

- Started with Information Assets
- Reviewed development and data warehouse
- Identified access management problems
- Information Classification Policy presented as standardization of terms
- *"If you say 'x classification', we'll understand how to protect your data." NOT "You must categorize your data before we accept it."*



## **Last word: Political Approaches**

- *...also not my specialty.*
- Following in the footsteps of the retiring lead
- Allying with unstoppable projects
- Finding a mentor who knows where the bodies are buried
- Very specific to each organization



## Discussion, Q&A

---

Jon Espenschied  
[jon@consciere.com](mailto:jon@consciere.com)

<http://www.consciere.com>





# More reading

---

- Edward Yourdon, *"Death March"* (ISBN 013143635X), originally published as...
- Edward Yourdon, *"Death March: The Complete Software Developer's Guide to Surviving 'Mission Impossible' Projects"* (ISBN 0130146595).
- NSA IATRP IA-CMM *"INFOSEC Assurance Capability Maturity Model"* ([http://www.iatrp.com/IA-CMMv3\\_1.doc](http://www.iatrp.com/IA-CMMv3_1.doc))
- NIST Special Publication 800-100 *"Information Security Handbook: A Guide for Managers"*
- NIST Special Publication 800-53 Rev. 3, *"Recommended Security Controls for Federal Information Systems and Organizations"* including Errata as of 09-14-2009