Choosing a Program Approach to HIPAA, GLBA, COPPA, NIST, NACSIM, and FDA Privacy and Security Requirements

Gary G. Swindon
President & CEO
G.Swindon Consulting

Once Upon a Time….Reactions to new Regulations

- SGAO!! (Shock, Grief, Anger, Outrage)
- You must be kidding!
- No one in their right mind would do this willingly.
- What will they think of next?
- Can we delay this? I don't want to deal with this now!

Swindon consulting

Regulatory Quiz

- 1. T/F The one year extension granted for the Transactions & Code Sets rule means:
  - A. That I have another year to work on it.
  - B. It applies to everyone.
- 2. T/F Bright orange is a fashion statement.
- 3. T/F The various regulations require me to buy the best security and privacy tools I can find.
- 4. T/F For HIPAA compliance I must obtain HIPAA compliant products to satisfy the requirements.
- 5. T/F COPPA is the short form of a famous restaurant name.

Swindon consulting

What is the Idea Behind all of These Regulations for Privacy and Security?

- To correct perceived improper behavior
- Create a programmatic approach to the issues
- Establish a minimum set of standards
- Develop a framework that can be measured and monitored

Swindon consulting

Regulatory Picture

- What and whose rules do you have to contend with?
  - HHS: HIPAA
  - DOD: NACSIM 5100
  - FDA: 21 CFR 11
  - HCFA: NIST 800
  - FTC: Existing Privacy Rules
  - EU and Safe Harbor

Swindon consulting

Common Threads in HIPAA, NACSIM etc.

- HIPAA is forever - as it turns out, so is the need for privacy and security
- Regulations tend to be policy based
- HIPAA is about business process, so are privacy and security
- Most regulations, including security require that measures be “cost effective”
- Apply common sense to compliance issues

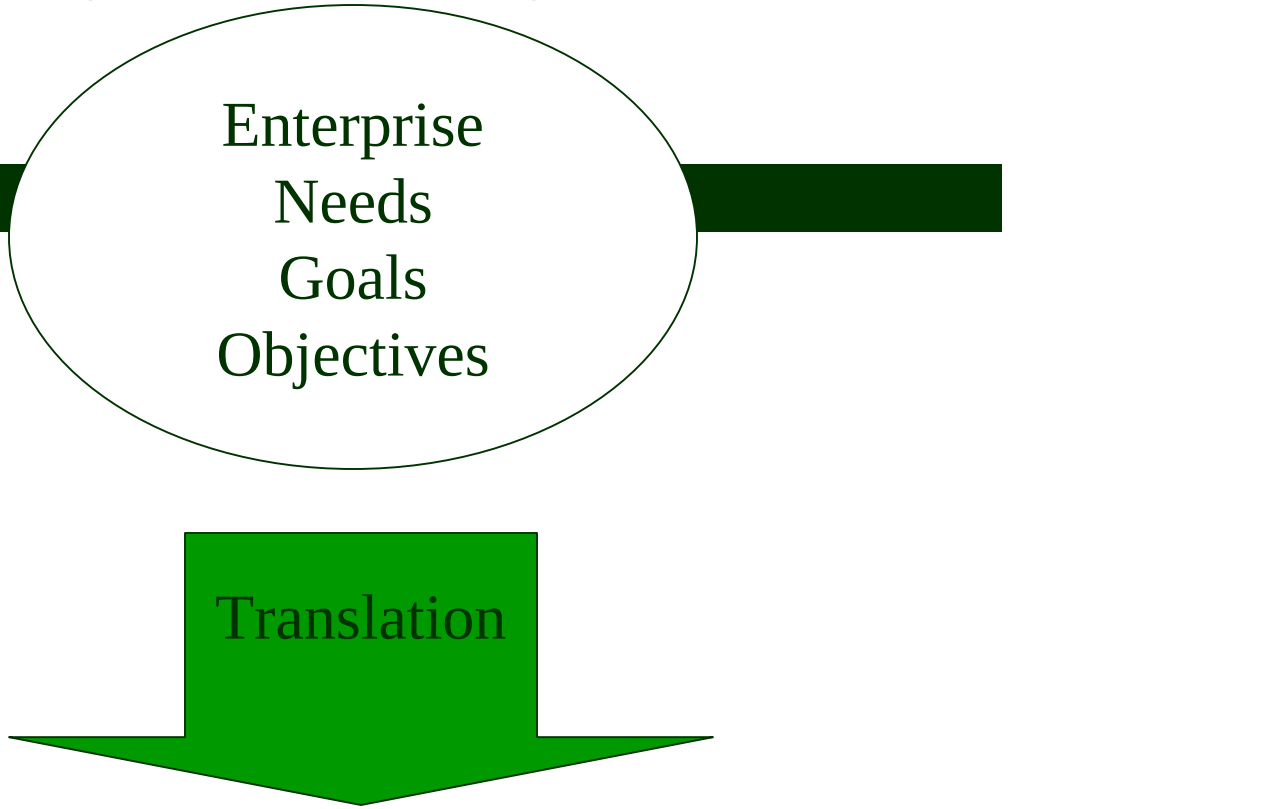
Swindon consulting

Applying the Common Threads to a Model

- Treat privacy and security as a common compliance theme
- Incorporate a “building block” approach
- Derive the privacy and security context from the business needs
- Reduce needs to the lowest common denominator

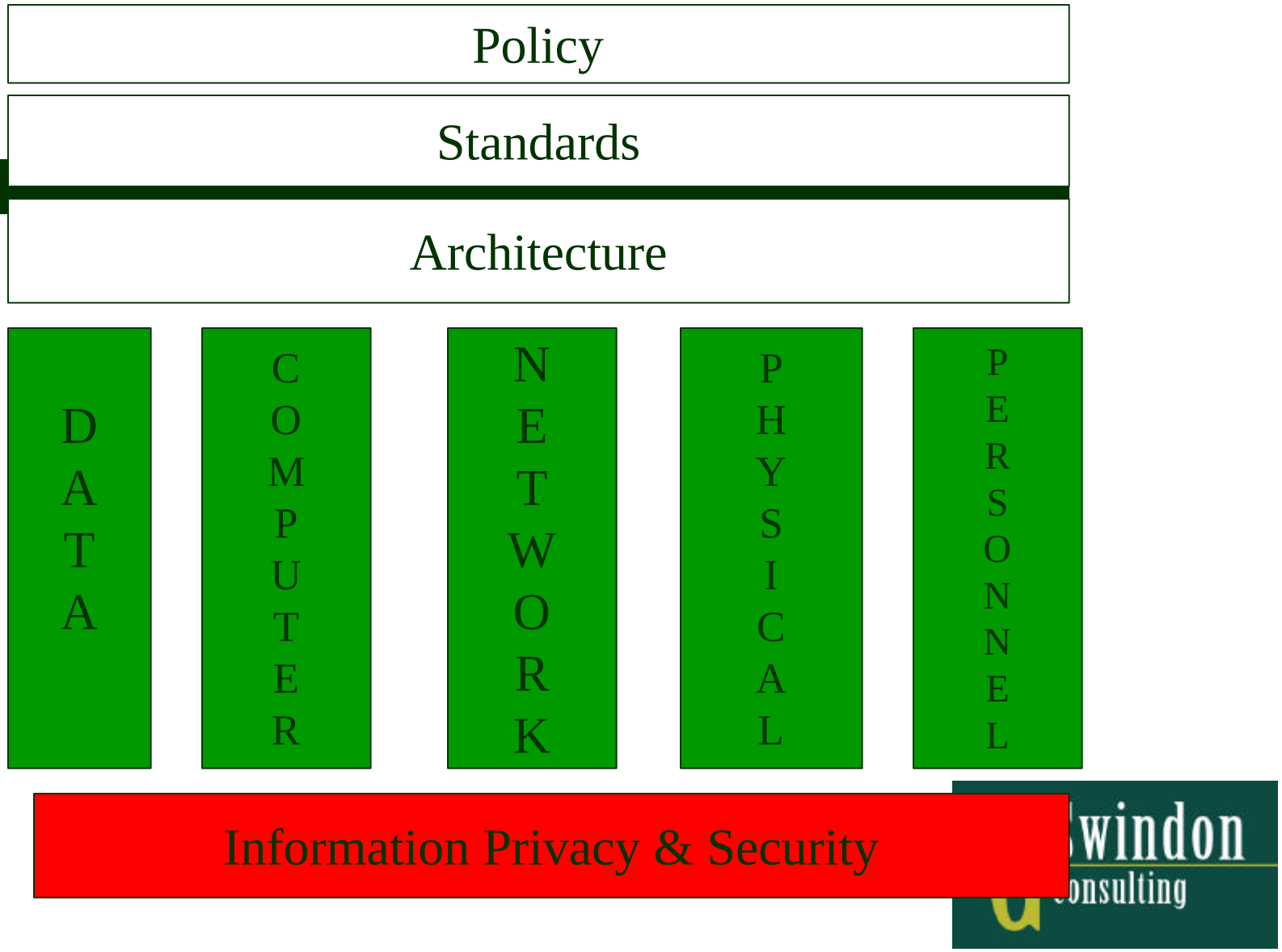
Swindon consulting

Privacy & Security Context



Swindon consulting

Privacy & Security Model



Policy

- Everything starts somewhere….
  - Ideally, it should be driven by the enterprise's needs
  - It should support the risk posture needed to achieve the trade-off or outcome desired
  - Better be clear enough to derive the standards to support it

Swindon consulting

Standards

- Whose??? DOD, NIST, FDA, HCFA….etc.
- Everything is a matter of degree; do you want absolute security and privacy of the information or will real world solutions be good enough?
- How much money do you have?

Swindon consulting

Architecture

- “The guts of the thing”
- Does it support the policy and can the standards be implemented without breaking the budget?
- Do the technical resources exist to manage it every day?
- The crossroads between resources and desire.

Swindon consulting

The Pillars of the Model

- Data-privacy and security while creating information for the business, customers and Business Associates
- Computer-securing the means to process store and retrieve data and information
- Network-the secure movement of data/information
- Physical-keeping all of the people, places, and things safe
- Personnel-enforcing the “need to know”

Swindon consulting

The Privacy & Security Model is used to:

- Determine the degree of flexibility needed to meet enterprise customer needs.
- Leverage competitive differentiators; i.e. trust.
- Determine investment levels in people and technology.
- Manage the organization's risk and exposure from internal as well as external sources.
- Secure the transactions that are the lifeblood of your business.
- Form the basis for any program regardless of the approach to compliance.

Swindon consulting

There are Three Basic Program "Flavors"

- The "program by accident" approach
  - We'll wait for the sanctions-extreme reaction
- The "bolted on" approach
  - Program gets added after the fact-react
- The "true cultural change" approach
  - Let's get everyone involved

Swindon consulting

Program by Accident

- Advantages:
  - Ignorance is bliss
  - Little initial cost
  - Almost no effort required except for planning for penalties

Program by Accident-cont'd

- Disadvantages:
  - Guaranteed to meet all kinds of new people
  - Data compromise is virtually certain
  - Penalties in the case of HIPAA could include being fitted for a bright orange jumpsuit
  - Virtually certain to attract the press sooner or later
  - No support from employees, in fact it may drive many of the good ones to someone else

Swindon consulting

The Bolted on Program

- Advantages:
  - Cheaper initial cost
  - Smaller initial effort
  - Requires little commitment from senior management
    - The “we have to do it” approach

Swindon consulting

The Bolted On Program-cont'd

- Disadvantages:
  - Much higher long term cost--HIPAA is forever
  - High risk of improper data exposure
  - High consequent risk of adverse publicity
  - Constant reaction to events
  - A major business distraction and nuisance
  - Constant demand for "out of cycle" resources
  - Little employee support or interest…another "toothache"

Swindon consulting

The True Cultural Change Program

- Advantages:
  - Less expensive long term
  - Risk of loss or exposure of data is minimized
  - Planning and execution is “owned” by everyone
  - Resources are generally preprogrammed and known quantities at the start
  - Allows leveraging the program for competitive advantage

Swindon consulting

The True Cultural Change Program-cont'd

- Disadvantages:
  - More front-end effort required
  - More initial resources required
  - Constant commitment of senior management required…lead by example…..or:
    - Program may revert to a variation of the bolted on approach

Swindon consulting

Operational Success Factors

- So how do we do this thing?
  - Decide whether the organization (senior management) believes that these regulations are permissive or restrictive
  - Make the decision which approach you want to use:
    - If restrictive, consider a bolted on or accidental approach
    - If permissive, use the cultural change model
    - Worst case; shoot for the cultural change model and settle (grudgingly) for the bolted on approach

Swindon consulting

Creating the Operations Environment for Culture Change

- Task organize:
  - Pick your best and brightest to lead the effort
  - Give them the functional help to determine what business opportunities might exist
  - Identify other personnel to work full time on the program
- Set the mission focus:
  - Clear and unambiguous

Swindon consulting

Operations-continued

- Create a separate business plan for the effort
  - Establish a separate budget for the effort
  - Identify the key milestones to commit resources
  - Metrics, metrics, metrics: if it can't be measured it doesn't exist
  - Track all costs until turn over to business unit(s)
  - Put a strong executive in the oversight role

Swindon consulting

Operations-continued

- Settle the fundamental issues:
  - Who “owns” the data?
  - Who is responsible for safeguarding the data?
  - At what point does the effort transition to the business unit(s)?
- Allow sufficient planning time
- Insure success (as much as you can) by putting other people’s “skin” in the game

Swindon consulting

Operations-continued

- Decide who gets/needs:
  - Education
  - Training
  - Awareness
- Decide communications techniques:
  - Intranet
  - Company bulletin
  - Ad campaign

Swindon consulting

Operations-continued

- Get outside help if needed
- Examine all parts of the business for regulatory impact
- Look at outsourcing some functions
  - Be honest with yourself on this one
  - Make sure you understand the true costs
  - Have someone check your assumptions

Swindon consulting

And for my Next Trick….

- Establish the “Business Associates Program”
  - Definitely get legal involved in this one
    - Specifies a contractual relationship between partners
    - Must contain an agreement on how both parties will protect data
    - Should provide for focused audits-not a license to go hunting
    - Must be as mutually enforceable as you can make it

Swindon consulting

Cut to the chase with an example- Technical Security

- Apply the program approach to this kind of problem as well as to business processes
- Don’t assume that the “techies” know what they are talking about
- Bring ALL interested parties to the table; IT, Privacy, Security, Business Unit(s), etc.
- Remember, you must live with what you create

Swindon consulting

Example-Technical Security

- HIPAA (and others) require that data be protected, hacks be prevented, management be proactive, etc.
- The IT architecture specifies:
  - Anti-virus
  - Intrusion detection
  - Asset control
  - Auditability

Swindon consulting

Example-Technical Security

- The business and legal folks require:
  - That it be policy based
  - That it not interfere with doing business
  - That it be auditable
  - That costs be contained
  - That it scale well as needs change

Swindon consulting

Example-Technical Security

- The IT organization wants to go out and buy tools to integrate to satisfy your needs
- Common sense dictates that that approach is probably not wise:
  - Tools seldom “talk to each other”
  - Each one has it’s own console for management
  - Each one requires it’s own training
  - Some require user intervention to work
  - The aggregate cost of a tools approach is prohibitive

Swindon consulting

Example-Technical Security

- Bottom line:
  - Reconcile business and IT needs
  - Look for a framework
  - Give consideration to solutions that are centrally managed and follow policy
  - Give consideration to solutions that protect existing investments and allow you to track and manage behavior

Swindon consulting

If all else fails….

- Look for someone else to blame
- It's a phase…the government isn't serious
- They'll never catch me…variation, they'll never take me alive
- I didn't want this job anyhow
- Does orange look good on me?
- I really prefer to live in Canada etc.

Swindon consulting

QUESTIONS ??

Swindon consulting