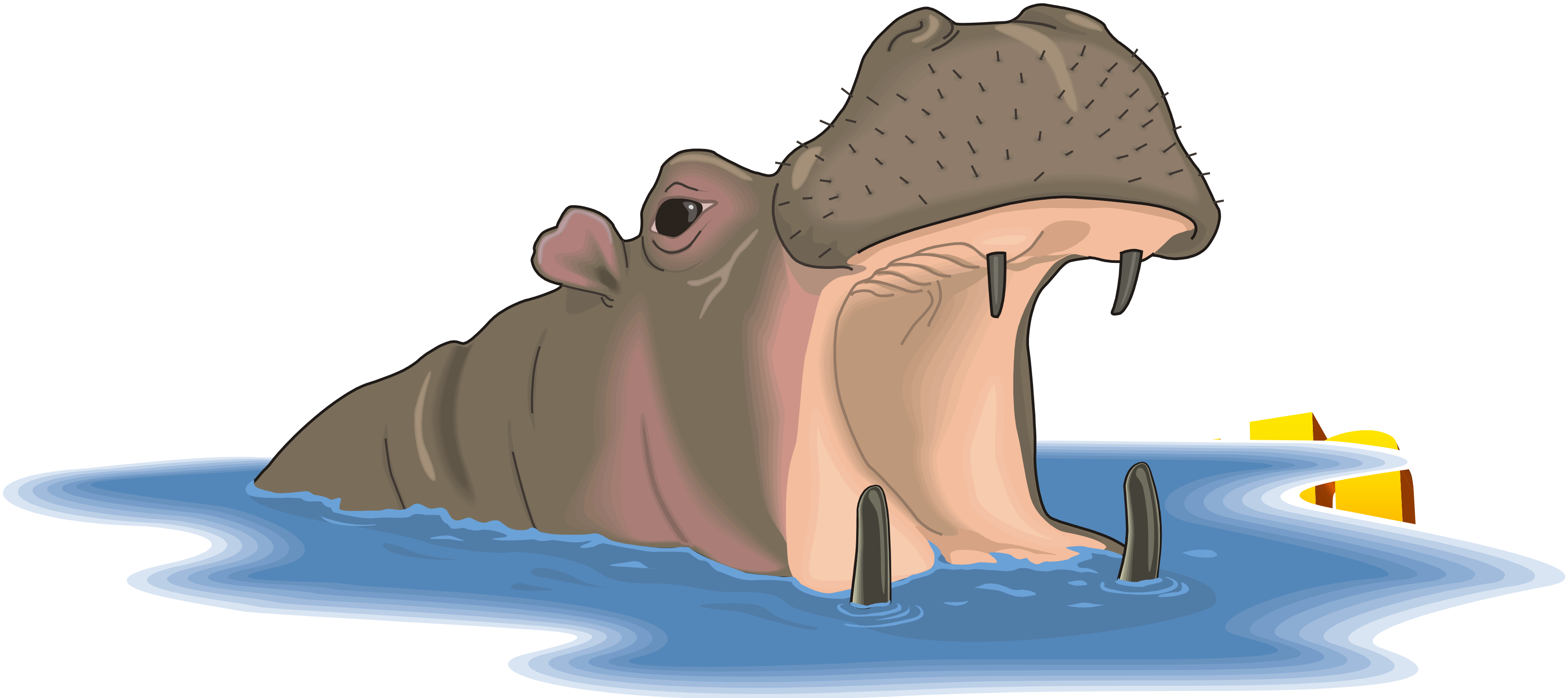
A Technical Template for HIPAA Security Compliance

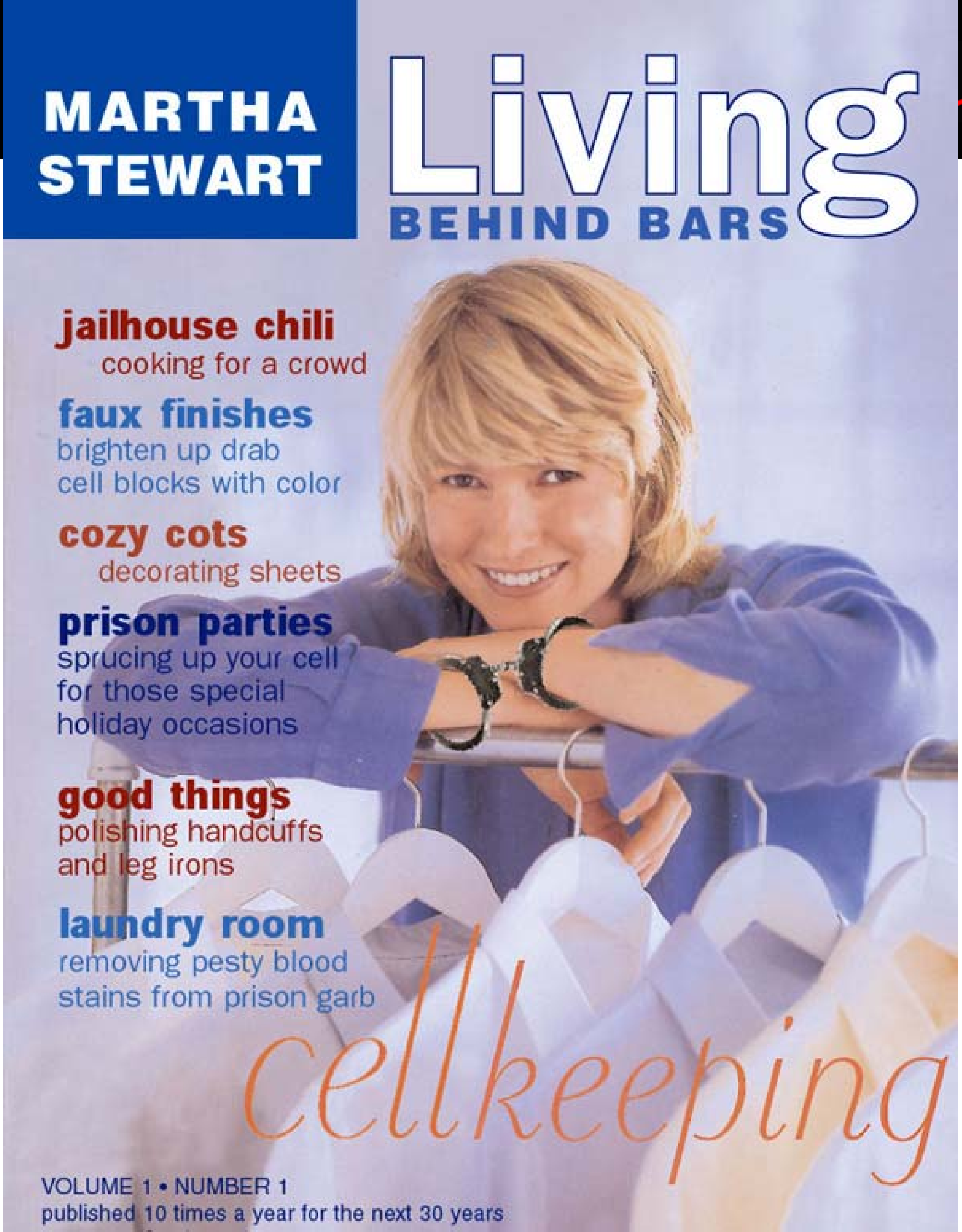
Peter J. Haigh, FHIMSS
peter.haigh@verizon.com

Thomas Welch, CISSP, CPP
twelch@sendsecure.com

Reproduction of this material is permitted, with attribution, for non-commercial purposes. This presentation represents the professional opinion of the authors. Verizon and Secure Enterprise Solutions accept no liability, expressed or implied, for the material contained herein.

Beware of the Hippo too!!





MARTHA STEWART Living

BEHIND BARS

jailhouse chili
cooking for a crowd

faux finishes
brighten up drab
cell blocks with color

cozy cots
decorating sheets

prison parties
sprucing up your cell
for those special
holiday occasions

good things
polishing handcuffs
and leg irons

laundry room
removing pesty blood
stains from prison garb

cellkeeping

VOLUME 1 • NUMBER 1
published 10 times a year for the next 30 years

Context - Privacy & Security under HIPAA

- Privacy is what you must promise to do, on or before 4/14/2003
- Security is about how you fulfil the promise on 4/14/2003, as well as 4/2005 (“stop-gap” security)
- Networks are how the authorized (and unauthorized) get PHI
- Improper network activity specifically identified as a “Security incident”
- Therefore network security is of paramount importance

Securing the Network

- **Sources of Security Threats**
  - Insiders/outsiders = 70/30, maybe 80/20
    - Malicious, dishonest, corrupt, distracted, disgruntled, negligent
    - Naturally curious, poorly trained, terminated
  - Terrorists
  - Hackers & Crackers
  - Computer criminals
- **Securing the Network Perimeter**
  - Outsiders & remote users
- **Policy, Training, Access Control, Monitoring, etc.**
  - Insiders
- **Beware of outdated or “crustacean” security**

State of the Art Security pre-Gunpowder!

What changed in the Final HIPAA Security Regulations?

- **Alignment with the Privacy Regulations**
- **Services & mechanisms = Technical Safeguards**
- **69 required implementation specifications (RIS) reduced to 13 (20 including subsections)**
- **22 addressable implementation specifications (AIS)**
- **New Definition of Electronic Media**
  - Voice (including voice-mail and video teleconferencing) & "paper to paper" fax not covered
  - Voice response & "faxback" are covered
  - What about Voice & Video over IP?
- **More regulations to come**
  - Electronic signature
  - Non-electronic PHI
  - Enforcement
- **But, no "evolving versions"**

What changed in the Final HIPAA Security Regulations?

- **Risk Analysis Vital!**
- **What is the Risk that (just a few examples):**
  - PHI can be used/disclosed inappropriately on:
    - Internet transmissions?
    - Wireless LANs?
    - Tele-worker Workstations?
    - Portable Devices (Hand-helds, PDAs)?
  - Passwords can be compromised?
  - Security incidents go undetected?
  - "Social engineering" will result in unauthorized access?
- **Document what you plan to do/not do, and why!**

Security Standards Matrix

- Administrative Safeguards
  - 12 Required
  - 11 Addressable
- Physical Safeguards
  - 4 Required
  - 6 Addressable
- Technical Safeguards
  - 4 Required
  - 5 Addressable

Note: The concept of "addressable implementation specifications" was introduced to provide covered entities with additional flexibility with respect to compliance with the security standard.

HIPAA v. ISO Standards

- Administrative Safeguards
  - Organizational Security
  - Information Security Policy
  - Personnel Security
  - Business Continuity Management
  - Compliance
- Physical Safeguards
  - Physical & Environmental Security
- Technical Safeguards
  - Asset Classification and Control
  - Access Control
  - Communications and Operations Management
  - Systems Development and Maintenance

Administrative Safeguards

Standards	Sections	Implementation Specification	R/A	T
Security Management Process	164.308(a)(1)	Risk Analysis	R	
		Risk Management	R	
		Sanction Policy	R	
		IS Activity Review	R	
Assigned Security Responsibility	164.308(a)(2)		R	
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	A	
		Workforce Clearance Procedures	A	
		Termination Procedures	A	
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	R	
		Access Authorization	A	**Y**
		Access Establishment and Modification	A	**Y**
Security Awareness and Training	164.308(a)(5)	Security Reminders	A	
		Protection from Malicious Software	A	**Y**
		Log-in Monitoring	A	**Y**
		Password Management	A	
Security Incident Procedures	164.308(a)(6)	Response and Reporting	R	**Y**
Contingency Plan	164.308(a)(7)	Data Backup Plan	R	**Y**
		Disaster Recovery Plan	R	**Y**
		Emergency Mode Operation Plan	R	**Y**
		Testing and Revision Procedure	A	
		Applications and Data Criticality Analysis	A	
Evaluation	164.308(a)(8)		R	
BA Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	R	

Physical Safeguards

Standards	**Sections**	**Implementation Specifications**	**R/A**	**T**
Facility Access Controls	164.301(a)(1)	Contingency Operations	A	
		Facility Security Plan	A	
		Access Control and Validation Procedures	A	**Y**
		Maintenance Records	A	
Workstation Use	164.310(b)	Documented procedures for system use	R	**Y**
Workstation Security	164.310(c)	Physical placement and control	R	**Y**
Device and Media Controls	164.310(d)(1)	Disposal	R	**Y**
		Media Re-use	R	**Y**
		Accountability	A	
		Data Backup and Storage	A	**Y**

Technical Safeguards

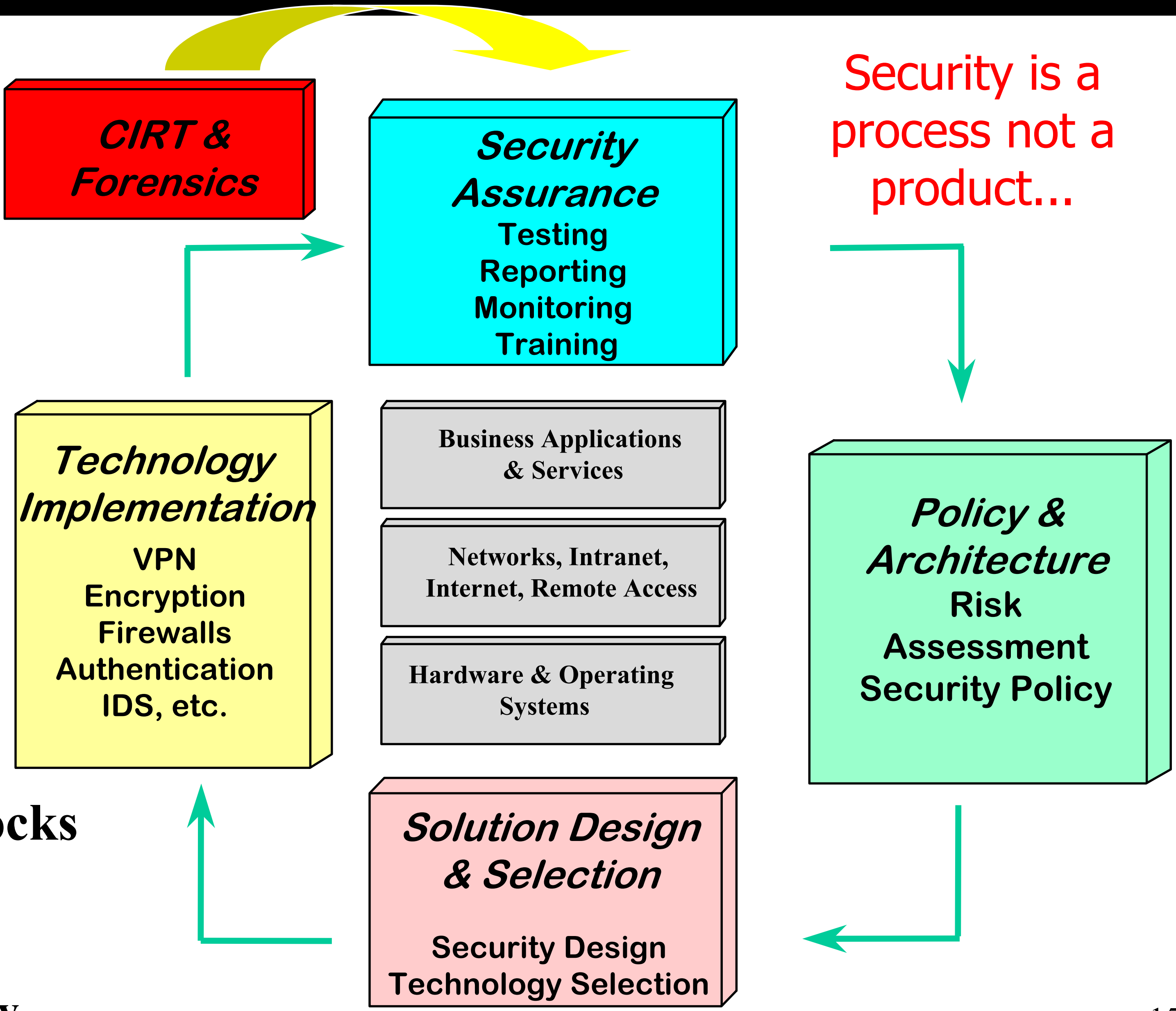
Standards	Sections	Implementation Specifications	R/A	T
Access Controls	164.312(a)(1)	Unique User Identification	R	**Y**
		Emergency Access Procedure	R	**Y**
		Automatic Logoff	A	**Y**
		Encryption and Decryption	A	**Y**
Audit Controls	164.312(b)		R	**Y**
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic PHI	A	**Y**
Person or Entity Authentication	164.312(d)		R	**Y**
Transmission Security	164.312(e)(1)	Integrity Controls	A	**Y**
		Encryption	A	**Y**

Steps to Technical Compliance

- **Conduct a Thorough Risk Assessment**
- **Evaluate the Risks**
- **Design a Secure Architecture**
- **Select & Implement Countermeasures**
  - Firewalls
  - IDS
  - Standardized hardware-software platforms
  - Host Hardening
  - Strong Authentication & Access Control (w/Auditing)
  - Integrity Controls (i.e. Tripwire)
  - Encryption and VPNs
  - Virus protection

- **Conduct Follow-up Audits (Quarterly)**
- **Establish Evidence that You’re “Doing Something”**
  - Waiting is Risky Business

Information Security Lifecycle

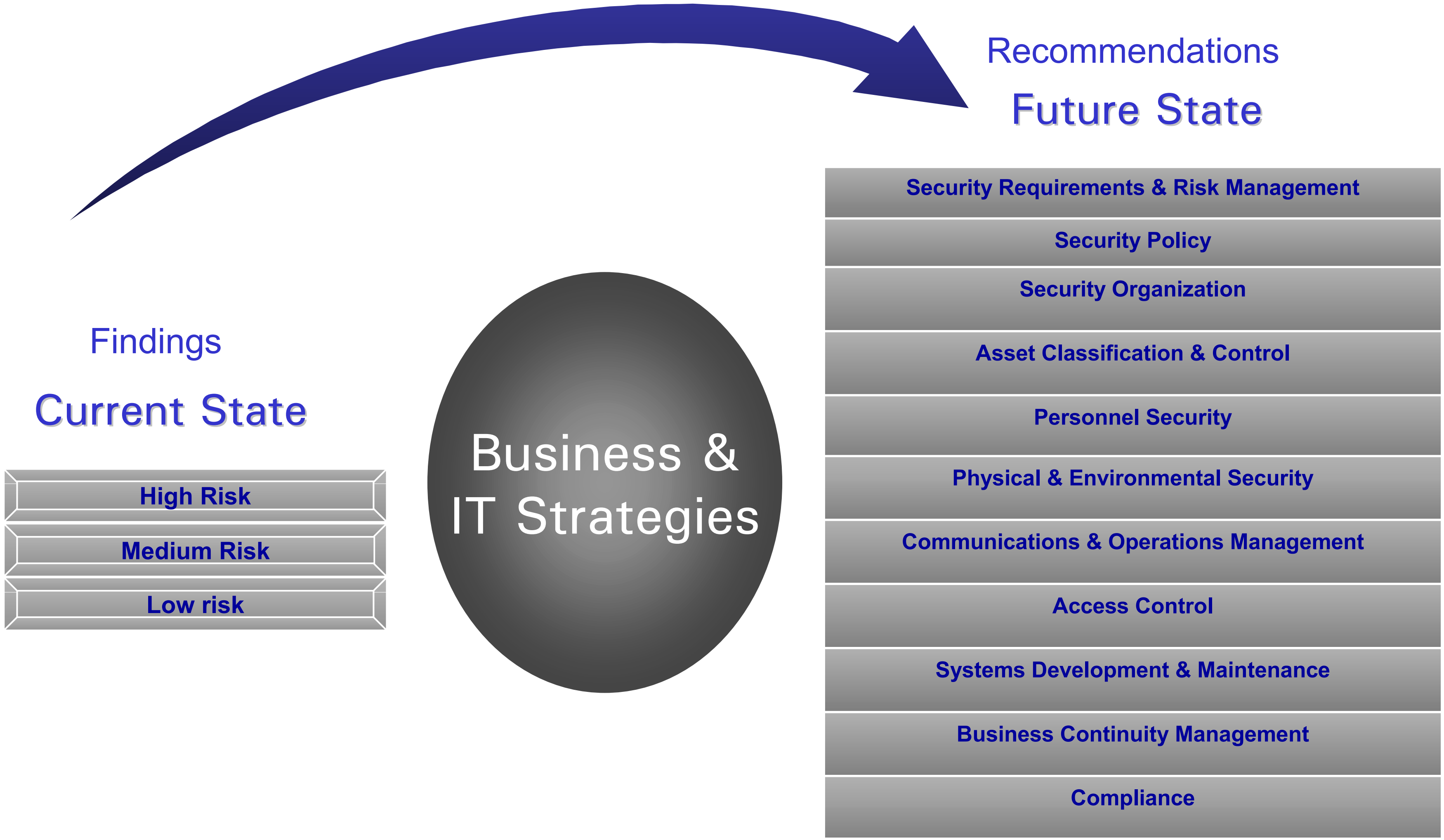


Security is a process not a product...

Building Blocks

- People
- Process
- Technology

Project Approach



Findings

Current State

High Risk

Medium Risk

Low risk

Business & IT Strategies

Recommendations

Future State

Security Requirements & Risk Management

Security Policy

Security Organization

Asset Classification & Control

Personnel Security

Physical & Environmental Security

Communications & Operations Management

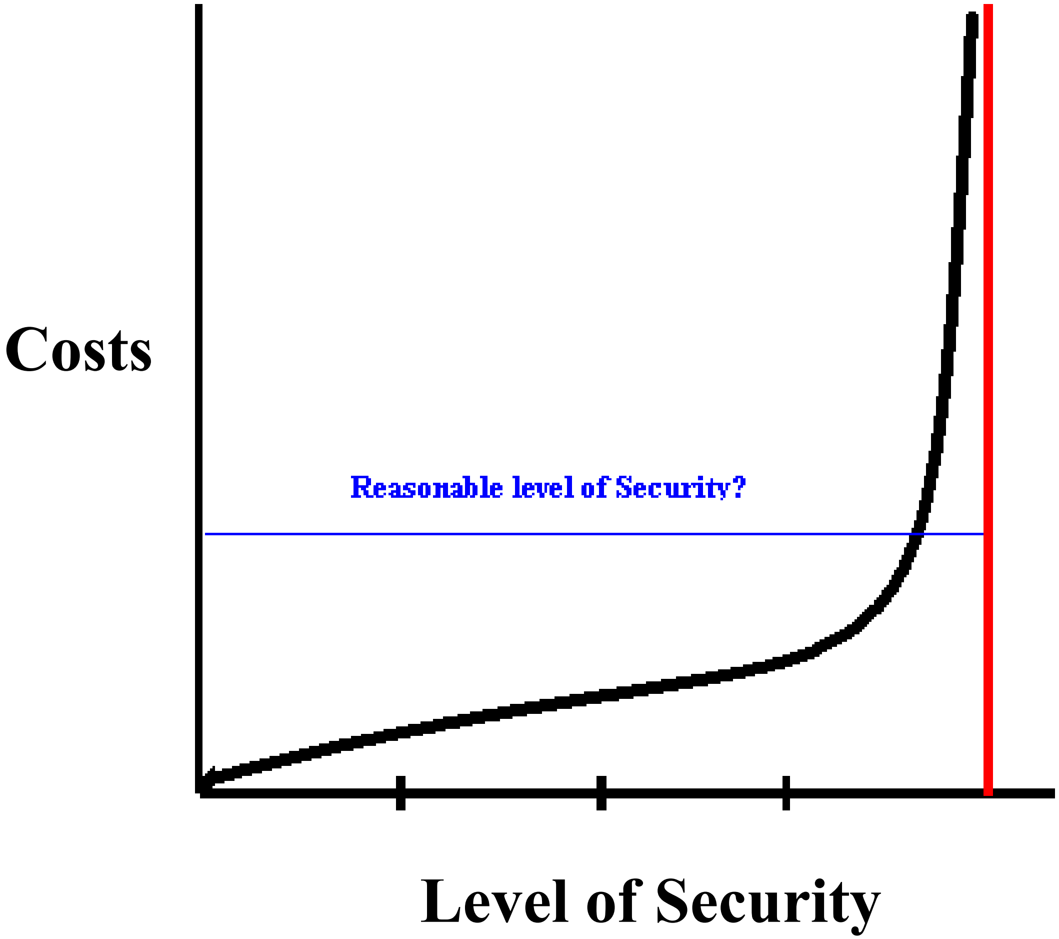
Access Control

Systems Development & Maintenance

Business Continuity Management

Compliance

Cost of Security



Be Prepared for an Attack

No one is immune!

…and the threat is increasing.

Technical Compliance Summary

- **Security is more than just a Login**
  - It MUST be implemented in layers
- **Security should be as transparent as possible**
- **An organization must be ready to:**
  - Protect
  - Detect
  - Respond… to any type of adverse event
- **The GOOD NEWS – many technical tools are available to improve security**

Can you hear me NOW?
JK