

Security Programs and Regulatory Compliance

Patrick C Miller, CISSP SSCP IAM
Interface2004 – Portland, OR
March 18th, 2004

BREAKWATER
BREAKWATER
SAFE HARBOR FOR YOUR BUSINESS



Information security

is a dynamic, constantly evolving, living system. Breakwater keeps ahead of the curve and anticipates threats to provide clients with highly responsive protection.



Presentation Overview

- **Breakwater Profile**
- **Current Situation**
- **Regulatory Landscape**
- **Security Program Roadmap**
- **Metrics and Framework**
- **Resources**

The logo features a photograph of a coastal landscape with a lighthouse on a cliff under a cloudy sky, set against a blue background.

Breakwater Security Associates

Information Security and Risk Management Services Firm since 1996.

A few of the things we do well...

- **Security Program Development**
 - Risk, Security and Vulnerability Assessments
 - Regulatory Compliance Gap Analysis
 - Policy Development and Auditing
 - Security Strategy
- **Managed Security Services**
 - Device Management
 - Event Correlation (Security Risk Management)
 - Monitoring
- **Training/Education**
- **Integration**



The Current Situation...

- Corporate Accountability and Fraud
 - Enron, WorldCom, etc...
 - Id Fraud
- Weak Economy
 - Fewer jobs overall
 - Pink slips = increased workload and frustration, as well as disgruntled employees
- Technology Shift
 - Automation (PCS), doing more with less
 - Ever-increasing complexity and power
- Terrorism
 - Can they use our people, processes, or technology against us?
- Lack of Expertise and Experience
 - Talent is scarce and “snake oil” is common



The Regulatory Landscape

***All of this means that
more regulations are
coming and we are
only seeing the tip of
the iceberg...***



Regulatory Avalanche

Why all the new regulations?

- The current situation...
- Most organizations **are not** implementing good security; many reasons for this
- Disagreement on what “good security” actually is or should be by industry working groups
- Unclear or lack of visibility into security within organizations by regulatory agencies
- Competing security standards that overlap or even conflict; very little coordination or centralization
- Industry self-regulation is getting bad press for not moving fast enough
- Technology has altered the risks; good timing
- *The Department of Homeland Security is just getting started (CII – 6CFR part 29)...*

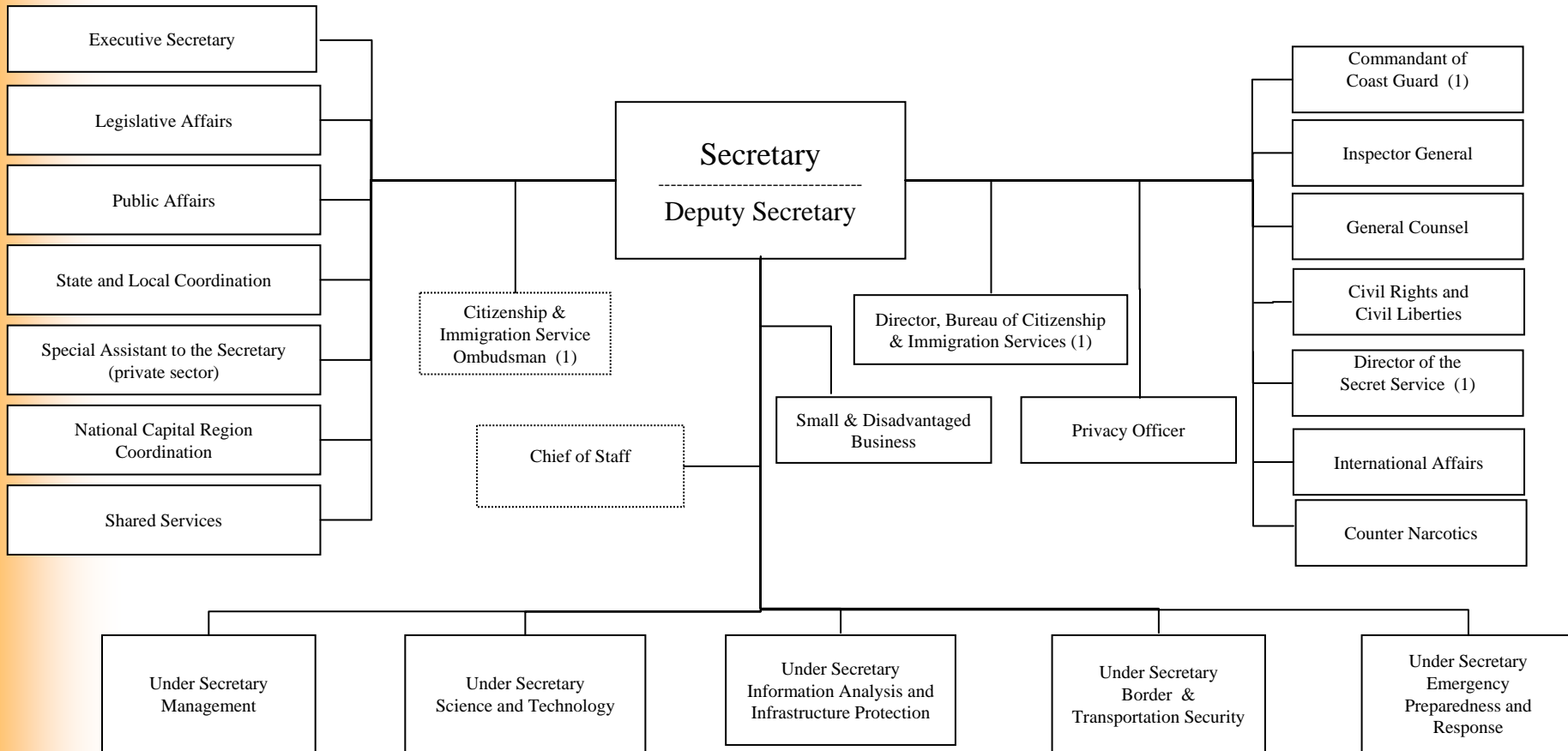


The DHS Umbrella

- **Border and Transportation Security**
 - The U.S. Customs Service (Treasury)
 - The Immigration and Naturalization Service (part) (Justice)
 - The Federal Protective Service
 - The Transportation Security Administration (Transportation)
 - Federal Law Enforcement Training Center (Treasury)
 - Animal and Plant Health Inspection Service (part)(Agriculture)
 - Office for Domestic Preparedness (Justice)
- **Emergency Preparedness and Response**
 - The Federal Emergency Management Agency (FEMA)
 - Strategic National Stockpile and the National Disaster Medical System (HHS)
 - Nuclear Incident Response Team (Energy)
 - Domestic Emergency Support Teams (Justice)
 - National Domestic Preparedness Office (FBI)
- **Science and Technology**
 - CBRN Countermeasures Programs (Energy)
 - Environmental Measurements Laboratory (Energy)
 - National BW Defense Analysis Center (Defense)
 - Plum Island Animal Disease Center (Agriculture)
- **Information Analysis and Information Protection**
 - Critical Infrastructure Assurance Office (Commerce)
 - Federal Computer Incident Response Center (GSA)
 - National Communications System (Defense)
 - National Infrastructure Protection Center (FBI)
 - Energy Security and Assurance Program (Energy)
- **US Secret Service**
- **US Coast Guard**

The DHS Org Structure

Department of Homeland Security





Current Regulations

To name a few of the current heavy-hitters...

- Sarbanes-Oxley (SOXA)
- GLBA
- HIPAA
- NERC 1200 UAS (FERC SMD)



A Closer Look...

First, a few points to note:

- This *is not* meant to be a comprehensive description of all current regulations
- This *is not* meant to be a debate on whether or not your organization is bound to any specific regulation
- This *is not* meant to be a discussion of the quality or effectiveness of any specific regulation
- This *is* a high-level overview of a select group of current and relative regulations



Sarbanes-Oxley

SOXA Overview

- Upper Management cannot take for granted the integrity of their financial reports, *or the systems that produce and store them.*

SOXA Rules

- Requires each annual report of an issuer to contain an “internal control report”, which shall:
 - state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
 - contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting
- Each issuer's auditor shall attest to, and report on, the assessment made by the management of the issuer
- Directs the SEC to require each issuer to disclose whether it has adopted a code of ethics for its senior financial officers and the contents of that code
- Directs the SEC to revise its regulations concerning prompt disclosure on Form 8-K to require immediate disclosure "of any change in, or waiver of," an issuer's code of ethics

GLBA Overview

- Privacy of “Customer” and “Consumer” Financial Data
- Privacy Track / Technical Track (501B)
- Adopted by Regulatory Agencies: OCC, Fed, FDIC, OTS, SEC

GLBA 501B Guidelines

- Create an Information Security Program
- Involve the Board of Directors
- Appoint a Security Officer
- Assess Risk
- Manage and Control Risk
- Oversee outsourcing arrangements (Vendor Management)
- Interpretive Guidelines created by the FFIEC



HIPAA

HIPAA overview

- Privacy, Transaction Code Sets, Security
- Applicable to “covered entities” (organizations that handle PHI – Personal Health Information)

HIPAA Security Rule

- Applicable to ePHI (electronic Personal Health Info)
- Compliance date is April 21, 2005
- Focuses on Administrative, Technical and Physical
- Certain requirements are “Addressable vs Required” meaning you have some choice around how and whether or not to comply (documentation a must!)
- NIST and ISO 17799 are normative standards
- Risk assessment, decision analysis, process/policy and documentation are very important



NERC 1200 UAS

NERC 1200 UAS Overview

- To reduce risks to the reliability of bulk electric systems from any compromise of critical cyber assets

NERC 1200 UAS Rules

- Focus on Administrative, Cyber and Physical
- Must define Critical Cyber Assets and Electronic Physical Security Perimeters
- Establish a single person in charge of security effort
- Report all Cyber Security Incidents
- Provide Incident Response, based on established guidelines
- Report regularly (quarterly to annually) to the “Compliance Monitor”
- Compliance required by Jan 1, 2005
- Currently, Process (Industrial) Control Systems are not in-scope, but will be in the upcoming NERC 1300



The Secret...

The secret to perpetual regulatory compliance?

Good security to start!

Don't wait for regulations to begin securing your organization, or you will always be behind

As usual, there is no "silver bullet" and the real solution is to actually do the hard work...



Get Involved

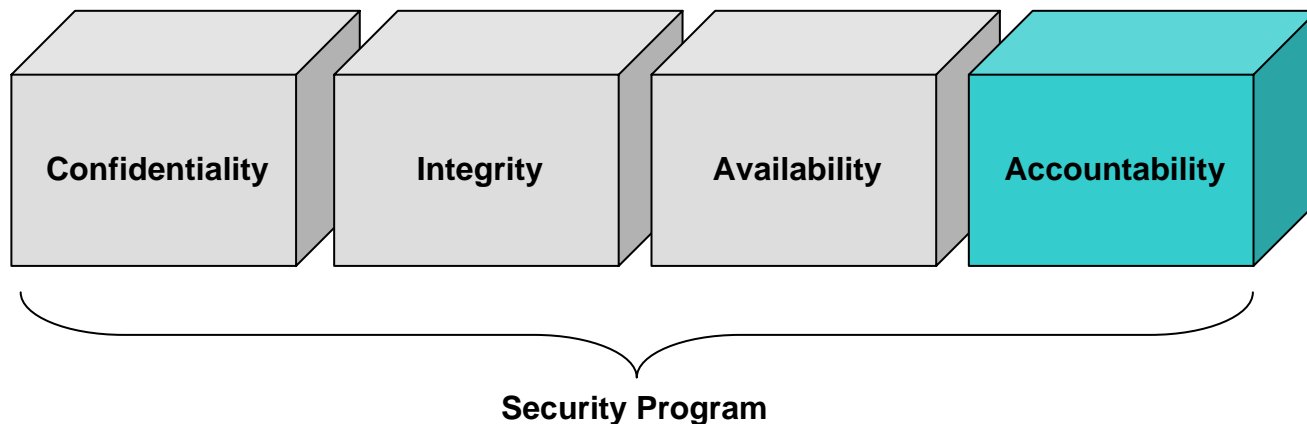
The real key is to be proactive...

- Minimize the “Ostrich Factor” - awareness
- Minimize the “Not Me Factor” - accountability
- Industry regulatory working groups
- Conferences and seminars
- Direct contact with regulatory agencies
- Provide a dedicated resource to drive compliance efforts
- Internal discussion within organization
- Get Executive awareness and support

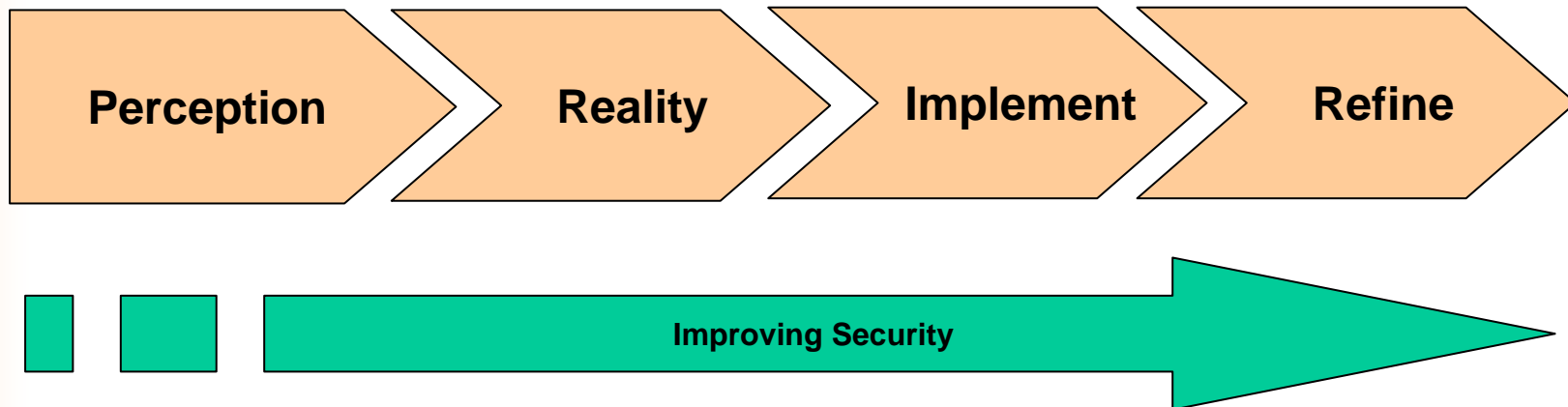
How can Security help?

- The environment is bad, very bad – but there are ways to succeed, safely and securely
- Many of the regulations and best practices strongly recommend the establishment/use of a dedicated security function for the organization
- What do you get with a dedicated security function?

The Goal:

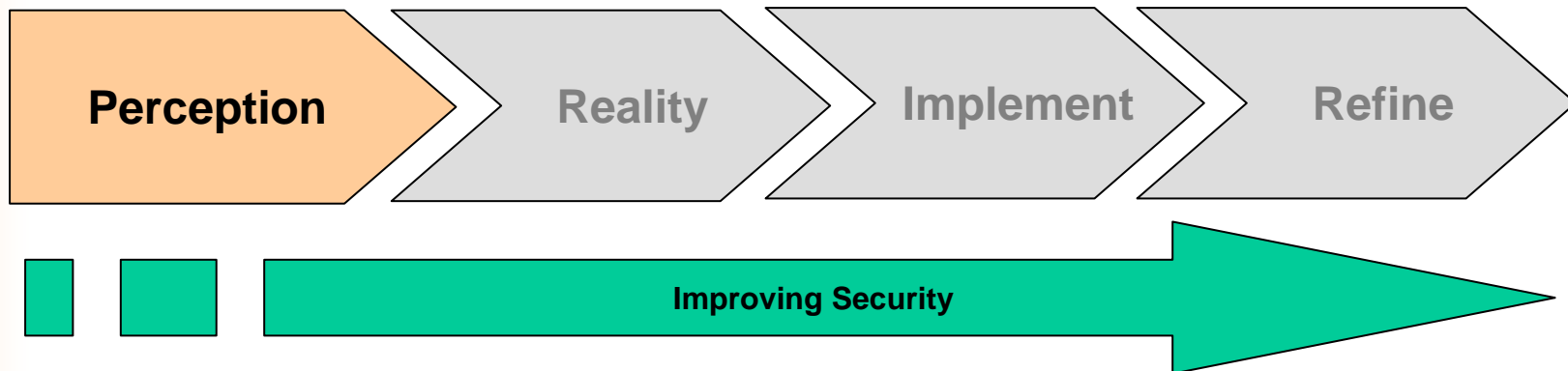


Security Program Concepts



- **Perception = Is security important?**
- **Reality = How bad is it?**
- **Implement = What to do and when?**
- **Refine = How to improve?**

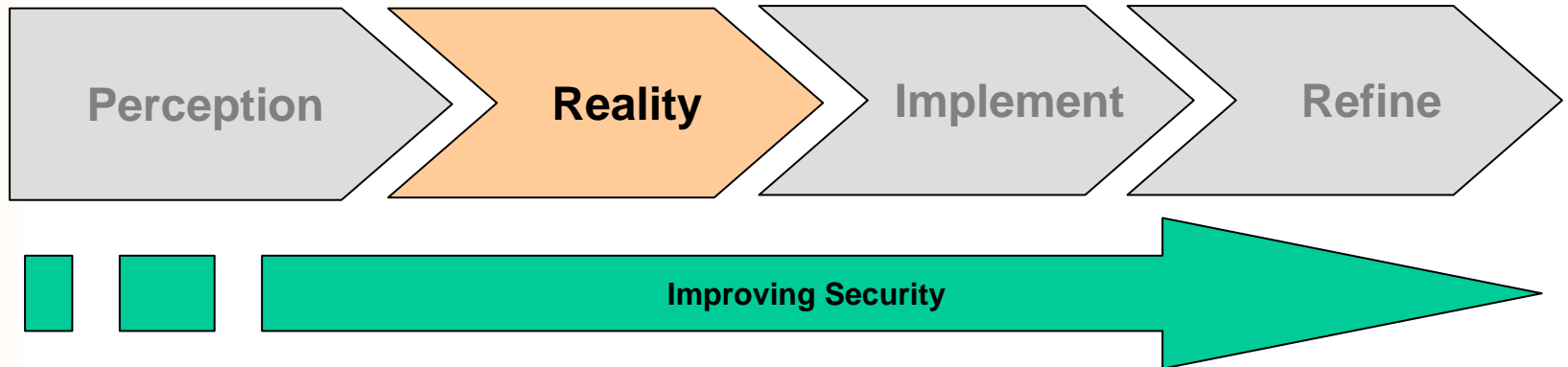
Security Program Roadmap



Start with Perception

- How does your organization perceive security?
 - Paranoia? Somewhat important? Part of everyday business?
- Take security seriously...
 - Obtain Executive-level support and direction; without it, good luck!
 - Establish a dedicated security function; put someone in charge
 - Ensure appropriate culture exists; awareness and training
 - Use real situations and real numbers; stay away from F.U.D.

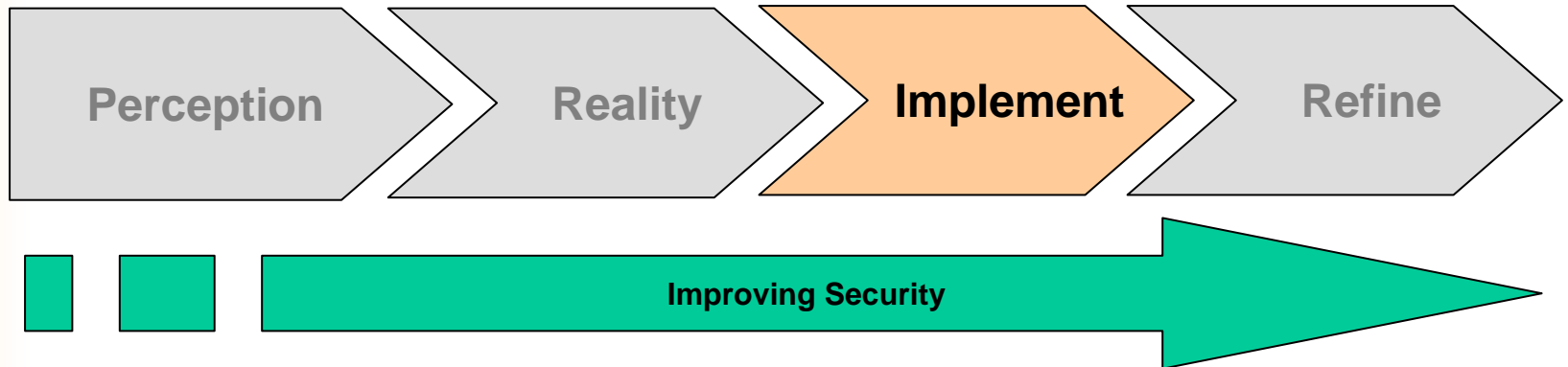
Security Program Roadmap



What Is the Reality?

- Assess the situation – how bad is it really?
 - Perform self-assessments before getting outside help, if able
 - Use repeatable and industry accepted methodologies (NIST, ISO)
- Present the information to Executives and Management
 - Again, stay away from F.U.D. and use “real” data (no hype!)
 - Schedule **regular** updates to Execs and Management
- Begin planning security efforts that map to immediate security concerns that also feed into the overall long-term strategy

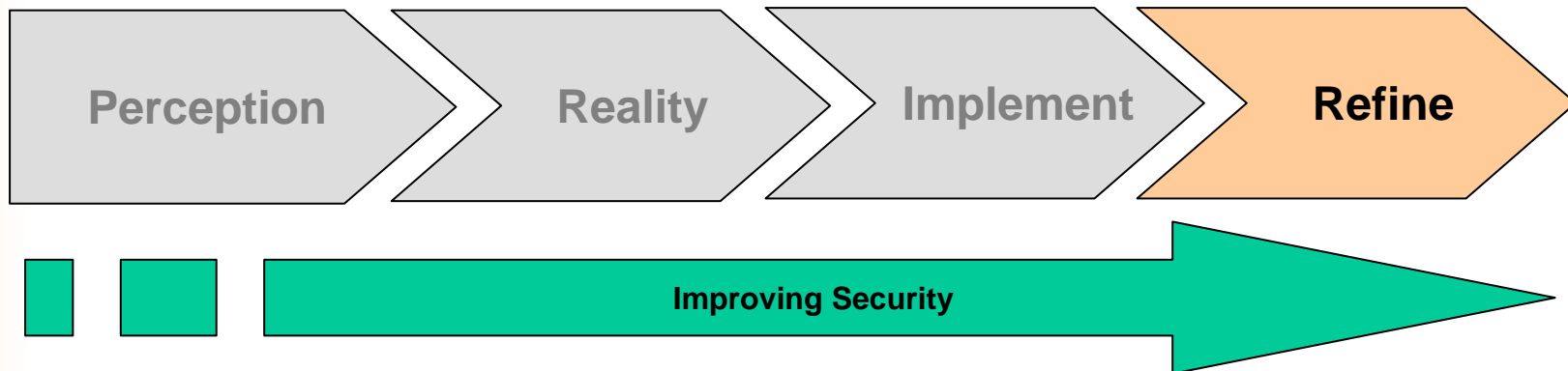
Security Program Roadmap



Implement Security Solutions

- Map security efforts to:
 - Business and Regulatory requirements
 - Realistic strategic goals
- Take action, and don't wait for your neighbor to do it first
 - Good security is forethought, not afterthought
 - Obtain appropriate funding, but don't spend too much
 - Hire or outsource experts; experience counts!

Security Program Roadmap



Refine Security Processes

- Measure everything!
 - Document deviation from Business and Regulatory requirements
 - Document deviation from tactical and strategic goals
- Adopt a sound framework for measurement
 - ISO 17799
 - ISO 21827
 - BSA Security Maturity Model
- Report relevant issues to Execs and Management regularly

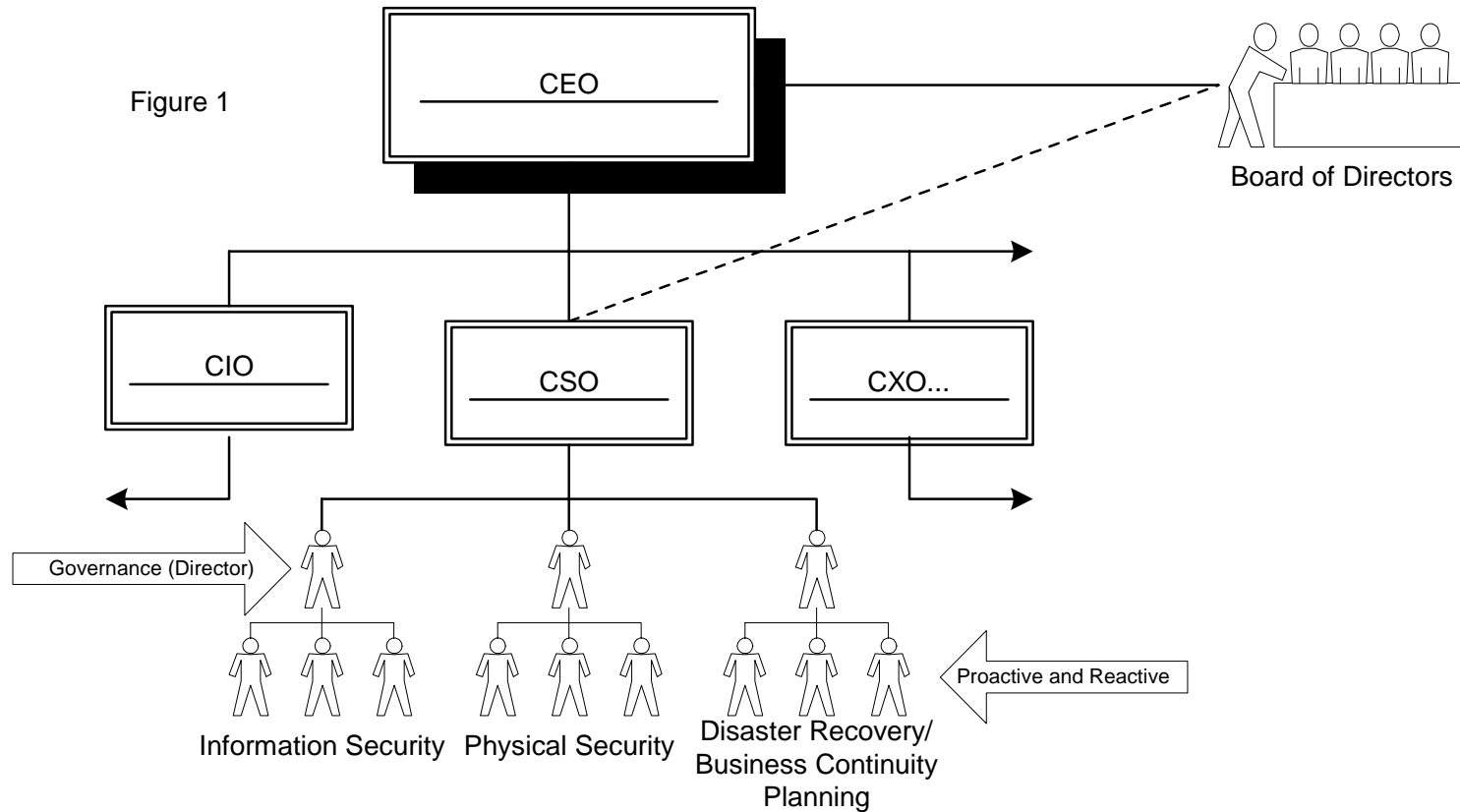


Security Program Components

- Security Management (Governance)
 - Authorization
 - Inter-organizational Communication
 - Policy
- Security Planning (Proactive)
 - Long-term Goals
 - Security Architecture
- Security Operations (Reactive)
 - Monitoring
 - Response

Best Practice Security Organization

Figure 1



Not the only option out there...



Security Program Priorities

- Risk (Assessment)
 - Determine just how bad it really is...
 - Start with biggest risks first
- Budget & Resources
 - Obtain the necessary resources to do the job
 - *May be the hardest task of all...*
- Compliance (Gap Analysis)
 - Where are you and where do you need to be relative to current and future regulations?
- Metrics and Benchmarking
 - Provide assurance that:
 - Security is being performed adequately
 - You are not only compliant to regulations today, but always



Security Program Metrics

- Measure your Security over time (show ROI)
 - Patch/vulnerability management
 - Malicious code (virus, worm, etc) management
 - SPAM and inappropriate content management
 - Intrusion Detection (IDS) and Integrity Assurance alerts
 - ***Assessments, both self and external***
 - ***ISO/IEC 21827; Capability/Maturity***



Frameworks for Compliance

**So you are assessing and measuring
everything, now what?**

**Adopt a proven framework that is
repeatable and provides long-term
compliance assurance. A good
starting point is ISO 21827...**

CMM (ISO 21827) Framework

Process Areas:

- Groups of Base Practices
- Defined set of processes
- Collective in nature

Capability Levels:

- Phases of maturity
- Range of expected results
- Process oriented

	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Process Area 1	X	X	X			
Process Area 2	X	X	X	X		
Process Area 3	X	X	X			

The CMM Matrix

The Basic Model, applied...

Capability Levels...

Process Areas...

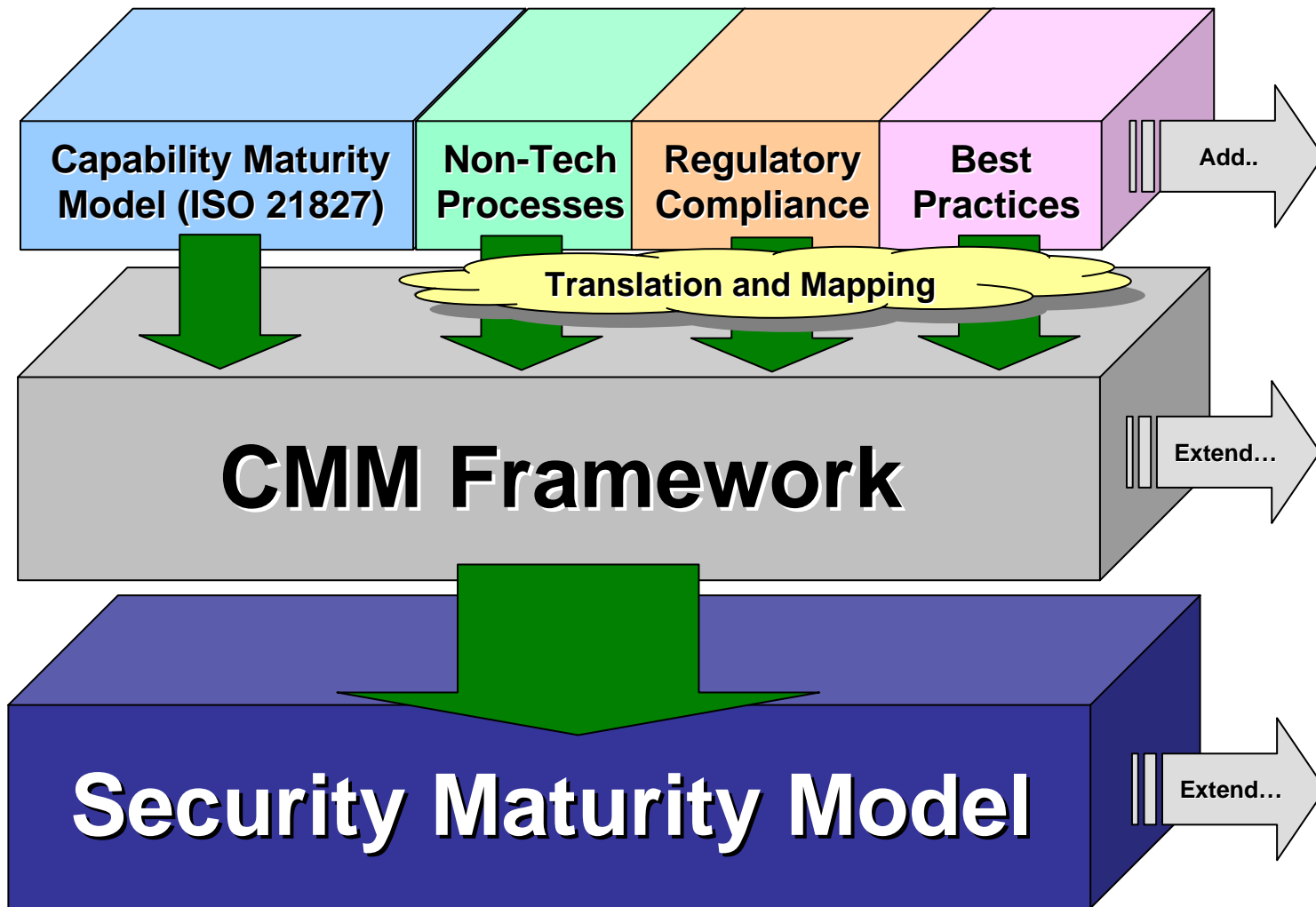
	Not Performed – 0	Performed Informally – 1	Planned and Tracked – 2	Well Defined – 3	Quantitatively Controlled – 4	Continuously Improving – 5
Administer Security Controls	X	X	X			
Assess Impact	X	X				
Assess Security Risk	X	X	X			
Assess Threat	X	X				
Assess Vulnerability	X	X	X			
Build Assurance Argument	X	X				
Coordinate Security...	X	X	X			



Flexibility in the Model

- **Process Areas are not finite**
 - Add organization-specific Base Practices
 - Add Regulatory Requirements
 - Add Industry Initiatives
 - Add Security Best Practices
- **Capability Levels are not finite**
 - Can be expanded to be more granular
- **Fully Customizable...**
- **CMM Framework is the core...**

Security Maturity Model Stack



Sample HIPAA CMM Summary

HIPAA Compliance Bar

"Reasonable and Appropriate"

High-Level HIPAA Administrative Security Maturity Summary

		Capability Levels				
		Not Performed – 0	Performed Informally – 1	Planned and Tracked – 2	Quantitatively Controlled – 4	Continuously Improving – 5
Security Process Areas	Security Management	X	X	X		
	Human Resource Management	X	X	X		
	Security Awareness Training	X	X	X		
	Operational Security	X	X	X		
	Security Incident Procedures	X	X	X		
	Contingency Planning	X	X	X		
	Policy Review	X	X	X		
	Administrative Security Maturity Score	2+				



The Overall Plan...

- Pay attention to the agencies and industry working groups for new regulations; get involved in the development of standards
- Get visibility, support and awareness of Executives and Upper Management
- Obtain the funding and resources to implement necessary security controls by presenting real data and measuring success
- Establish a compliance framework that supercedes most current regulations, such as ISO 17799 or 21827, but doesn't go too far beyond what is appropriate



Useful Links...

Sarbanes-Oxley Act (SOXA)

- <http://www.sec.gov/divisions/corpfin/faqs/soxact2002.htm>
- http://www.sarbanes-oxley.com/displaythread.php?message_id=2808&forum=news
- <http://www.sarbanes-oxley-forum.com/>
- <http://www.amrresearch.com/SOA/SarbanesFAQ.asp>
- http://www.arma.org/legislative/sarbanes_oxley.cfm
- <http://www.softlanding.com/sox/docs/sox-faq.pdf>
- <http://www.qndt.com/far/sarbanes.asp>

Gramm-Leach-Bliley Act (GLBA)

- <http://www.ffiec.gov/>
- http://www.protectinfo.com/safeguards_faq.aspx
- <http://www.secnap.net/glba/FAQ.doc>

Health Insurance Portability and Accountability Act (HIPAA)

- <http://aspe.hhs.gov/admnsimp/faqtz.htm>
- <http://aspe.hhs.gov/admnsimp/index.shtml>
- <http://www.rx2000.org/KnowledgeCenter/hipaa/hipfaq.htm>
- http://www.hipaadvisory.com/action/faqs/faq_main.htm

NERC 1200 Urgent Action Cyber Security Standard (NERC 1200 UAS)

- <http://www.esisac.com/library-guidelines.htm>
- <http://www.nerc.com>
- <http://www.breakwatersecurity.com/energyandutility/>

The Department of Homeland Security

- <http://www.nipc.gov/dailyreports/dailyindex.htm> - DHS IAIP Daily Report
- <http://www.dhs.gov/dhspublic/display?theme=10> – Grants from the DHS
- <http://www.dhs.gov/dhspublic/display?theme=13&content=3345> – Organizations within the DHS



Questions?

Patrick C Miller, CISSP SSCP IAM

Senior Security Consultant;

Energy and Utility Practice Principal

pmiller@breakwatersecurity.com

503.517.3407 (desk)

503.312.0703 (mobile)