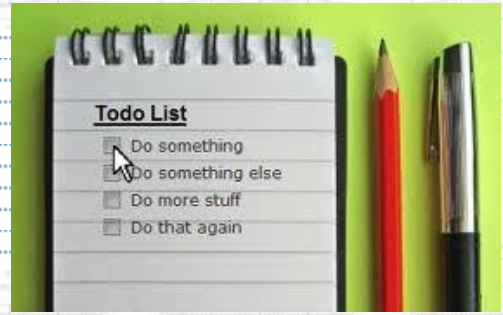
BUILDING BRIDGES

Security Metrics to Narrow the Chasm Between Perception and Reality

Brian A. Engle
CISO, Texas Health and Human Services Commission

Agenda



- In the beginning…
  - What created the perception chasm?
  - Contributing factors that widen the chasm
- Truth, Fact and Reality
  - Primary support materials to bridge the gap
  - Construction elements and design
- Where can the bridge take us…
  - Practical uses and worthy destinations

Speaking in tongues

Ponemon Second Annual Cost of Cyber Crime Study

Viruses, worms, Trojans	==>	100%
Malware	==>	96%
Malicious Code	==>	42%

- Virtually all organizations experienced attacks relating to **viruses, worms and/or trojans** over the four-week benchmarking period. Ninety-six percent experienced **malware** attacks, 82 percent experienced **botnets**, 64 percent experienced Web-based attacks, 44 percent experienced stolen or hijacked computing devices, 42 percent experienced **malicious code**, and 30 percent experienced malicious insiders.
- Footnote - Malware attacks and malicious code attacks are inextricably linked. We classified malware attacks that successfully infiltrated the organizations' networks or enterprise systems as a malicious code attack.

The Bigger Picture

- Standards interpreted and implemented with tribal inconsistency
- Regulations, laws, auditors and compliance requirements
- Qualitative risk math in vivid Technicolor
- Voodoo and Magic Fairy Dust
- Personality based bias and trust
- The “End of the World” as we know it vulnerabilities
- Misguided faith in legacy protection and various technologies

Virtualization

Mobility

Social Media

CLOUD

APT

Cyber

<InsertTermHere>

threat war terrorists activists
hacktivists
cybercybercybercyber

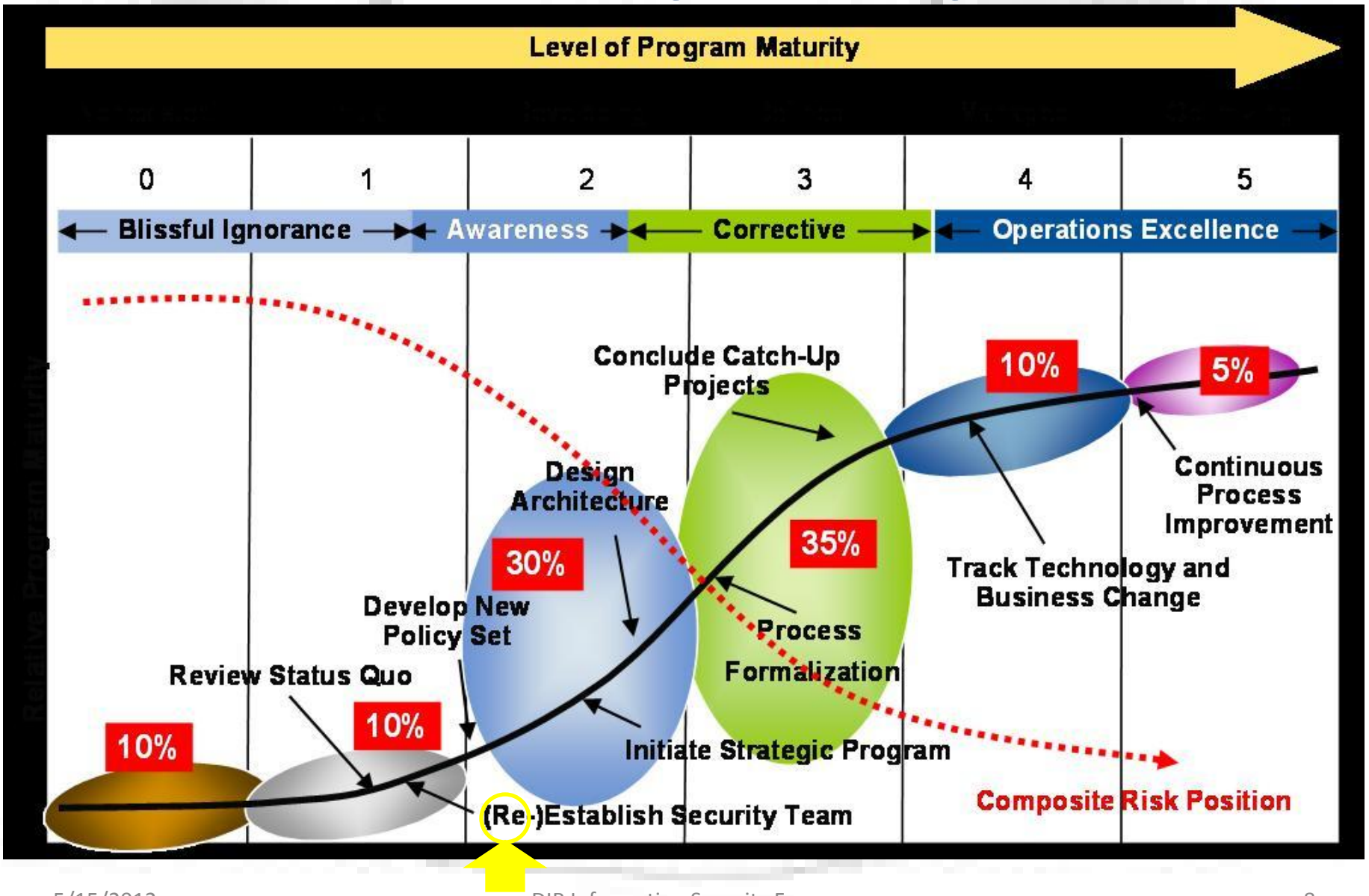
Consumerization

You want me on that wall…
You need me on that wall…
What happened to the wall?

Executive Dashboard Financial Metrics

- Investment metrics do not validate security
  - ROI for Security?
  - Cost Avoidance?
  - Insurance Comparisons
- % of Security Spend Compared to Overall IT Spend
  - Comparative, but irrelevant
- **Consider % of Security Spend Compared to Overall Company Expenditures**

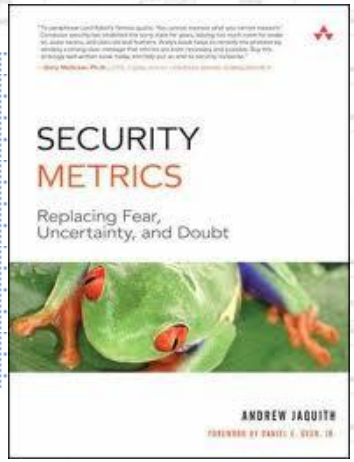
Gartner Security Maturity Model



So close, yet so far away…


THE VISIBLE OPS HANDBOOK
IMPLEMENTING ITIL IN 4 PRACTICAL AND AUDITABLE STEPS
Revised 1st Edition
IT Process Institute
KEVIN BEHR, GENE KIM AND GEORGE SPAFFORD
VISIBLE OPS SECURITY
ACHIEVING COMMON SECURITY AND IT OPERATIONS OBJECTIVES IN 4 PRACTICAL STEPS
IT Process Institute
GENE KIM, PAUL LOVE AND GEORGE SPAFFORD
Tom McHugh/Photo Researchers, Inc.

Jaquith's Laws of Metrics



- Consistently measured without subjective criteria
- Expressed as a cardinal number or percentage, not qualitative
- Expressed using at least one unit of measure
- Contextually specific / relevant such that they are actionable
- ***Cheap to gather***

3 "*Simple*" Metrics

1. What you do
   - and conversely what you don't do
2. The effectiveness, maturity and breadth of coverage of what you do
3. The risk that is in the remainder of the factorable computation of 1 and 2

Truth, Fact and Reality

- What you do
  - How well is it working? (effectiveness)
  - Are you doing it everywhere you need to be? (scope/depth/breadth)
  - Can you continue doing it consistently? (maturity)
  - How much does it cost?
- What you don't do
  - Dig for the denominator

What you do

- People, Process and Technology
- Activities, Functions and Interactions
- Objectives, Outputs and Oversight
- Technological countermeasures and defenses

= Controls

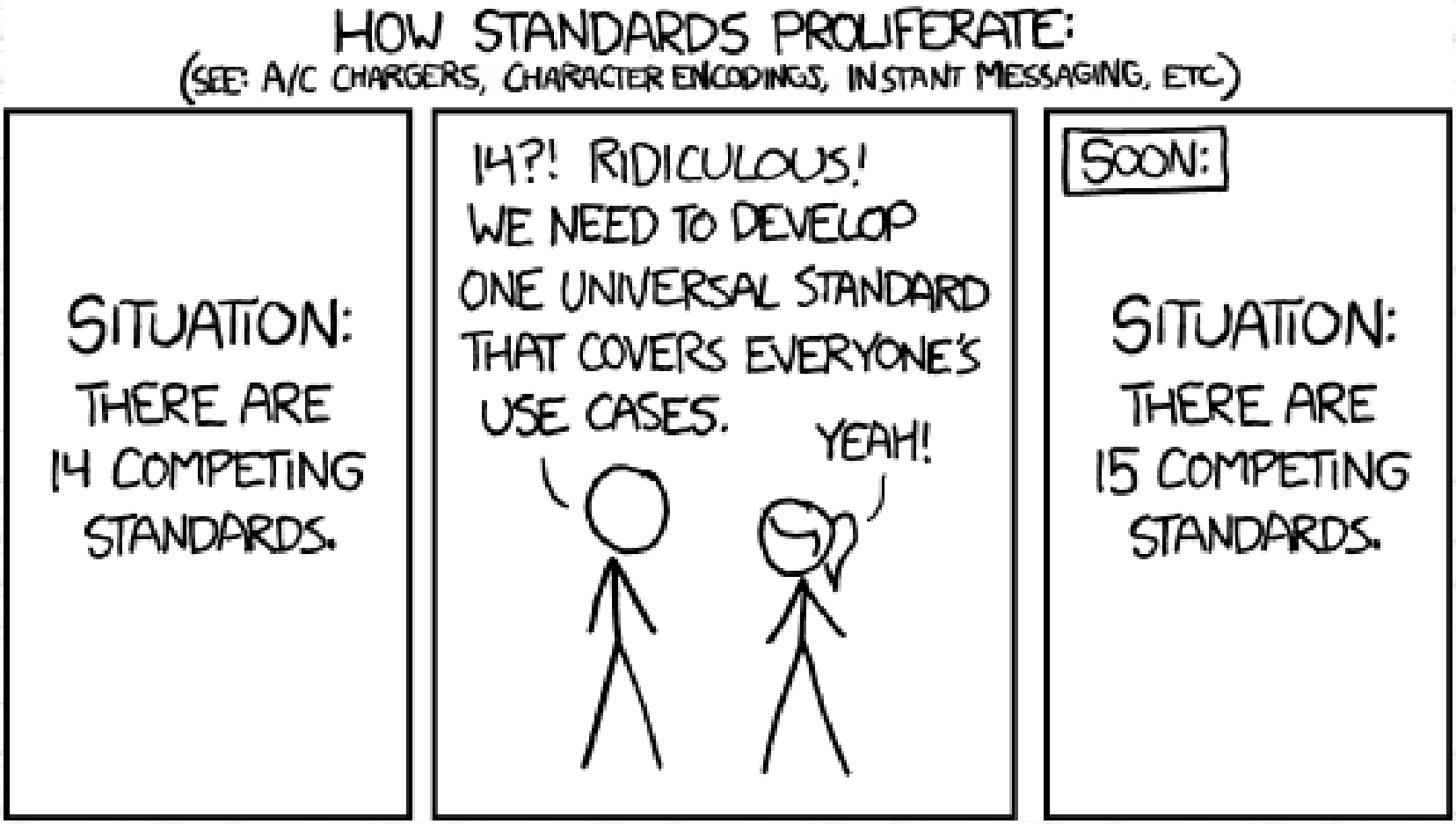
Metrics

- X out of Y ***Mandatory*** Compliance Control Activities Implemented
  - Performed, costing $$
  - Leaving a remainder of $$ for additional protection control activities
  - Requiring T time to implement new activities
    - Managing audit findings and planning v. scheduling program activities

Metrics

- X out of Y *Required* Control Activities Implemented
  - Applied across Z scope
  - # Performed at E rate of effectiveness
  - # Performed below E rate of acceptable effectiveness
  - Time to remediate ineffective processes

Not another standard



Control Frameworks

Framework, Standard or Regulation	Segmentation	Defined Controls
NIST 800-53 (v3 Moderate)	26 Families	228
ISO 17799 / 27002	12 Sections	140
1 TAC 202 Title 1 Part 10 Chapter 202	9 Subsections	110
COBIT	5 Generic Process Guidance 37 High Level Outputs	Metric Boatload
PCI	12 Requirements	211

Control Effectiveness, Scope, and Maturity

Objective	Defined Control	Scope / Depth	Effectiveness	Maturity CMM	Cost	Crosswalk Connections	Owner / Division / Region
AC	Provision Account	Specific or Groups of Apps	90%	Optimizing	$$$$	1TAC202Ref HIPAA Req IRS 1075	
AC	De-provision Account	Specific or Groups of System	25%	Ad-Hoc	$$$$	Standards, Compliance Requirements	
AC	Grant Access Priv.	Function role or org	75%	Repeatable	$$$$	Standards, Compliance Requirements	
AC	Revoke Access Priv.	{SOX |PCI | HIPAA} Systems	25%	Defined	$$$$	Standards, Compliance Requirements	

Operational Control Metric Dashboard

Physical and Environmental Protection (PE)

Access Control (AC)

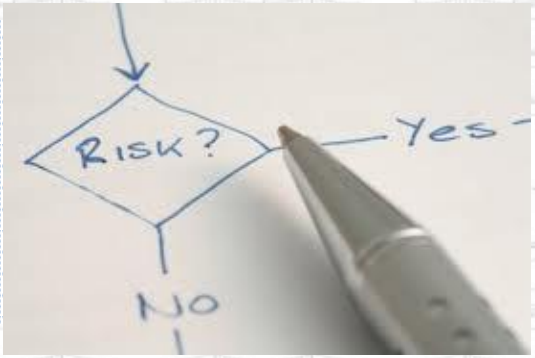
Configuration Management (CF)

Incident Response (IR)

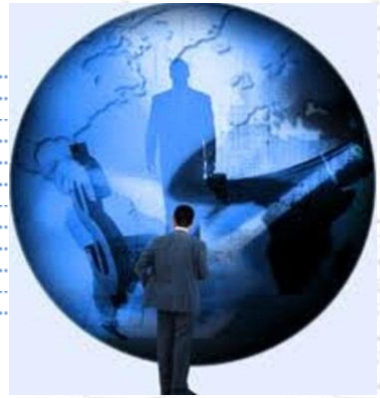
Digital Media Protection (MP)

Personnel Security (PS)

Evaluating Residual Risk

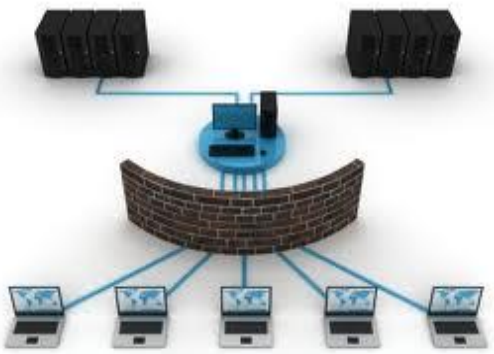


Where Does the Bridge Lead?



- Internally
  - Actually answer the “Are we secure” question
  - Provide a sustainable program framework
  - Provide consistency (staff and management)
- Externally
  - Establish accountability and assurance

Where Can the Bridge Take Us?



- Outsource Providers
  - Trust but **VERIFIED**
  - To the cloud on more than a wing and prayer
- Security Product Vendors
  - Ingredients and functions of security program

(Silver Bullets and Assorted Fairy Tales)

Summary

- There is a gap in the ***perception*** of security and the ***reality*** of what is provided
- It takes a lot of ***effective*** activities that come at a cost to narrow the gap
- Articulating the ***size*** of the gap is difficult
- Closing the gap with ***truth*** and ***fact*** is costly, but absolutely ***necessary***

About…

Capitol of Texas ISSA

The preeminent trusted global information security community

http://www.austinissa.org @austinissa

COMMUNITY -- KNOWLEDGE -- LEARNING -- CAREER

HHSC

HHSC oversees the operations of the health and human services system, provides administrative oversight of Texas health and human services programs, and provides direct administration of programs.

$30B/Year - 200 programs - 56,000 Employees – 1,000 locations - 5 agencies

Serving the citizens of Texas

Teach Security, Teach Christ; Teach Security In Christ

http://www.hackformers.org @hackformers

Thank You!

Questions?

Contact Info:

Brian.Engle@hhsc.state.tx.us

@brianaengle


Add clarity…
Not cloudiness.
Engineer Good Security
Let’s start building some bridges.