

!mpactmakers

Better Business. Better Community.

Information Security Program Maturity, Metrics ... and Taking it to the Next Level

Cathie Brown, CGEIT, PMP, CISM, CISSP



Presentation Summary

Topic: Information Security Program Maturity and Metrics

Synopsis: This presentation will focus on assessing security program maturity using the NIST PRISMA (Program Review for Information Security Management Assistance) maturity model and the role of security metrics to increase the overall program maturity. It is not just about having policies and tools. Maturing the program takes a change in the culture to actually implement processes, raise awareness and share information among all stakeholders.

- Why measuring the maturity of your security program is important
- How to use the PRISMA model to measure maturity of your program
- How metrics play a role in measuring and increasing the maturity of the program
- The difference between 'absolute' metrics and relative 'metrics' and why both are important

PRISMA

Agenda

- Speaker Introduction
- Maturity
- The Journey
- What is PRISMA?
- How this works
- Metrics
- Final thoughts
- Q&A



Speaker Introduction

About me...

- Principal Consultant, GRC Practice Lead and CISO for Impact Makers
- Maintain certifications as PMP, CGEIT, CISM, CISSP
- Experience as employee and consultant
 - state government
 - healthcare
- Past ISACA VA Chapter President, Board Member
- Previous President and Current member of Region 2000 Technology Council
- Speaker – ISACA, HIMSS, TechEdge...
- COV Citizen, Licensed Driver, Birth Certificate, Own property, Have a Speeding Ticket(s), File taxes, Patient in healthcare systems, Banking Customer...
- Enjoy Facebook, LinkedIn, Twitter...



Maturity

How has your program changed in 10 years?

- The Commonwealth Information Security Standards (COV ITRM SEC 501) will be 10 years old this July!
- **TEN YEARS!!!**
- Does your agency have a Culture of Security?
 - ✓ Current, documented information security policies
 - ✓ Documented procedures developed from the policies
 - ✓ Procedures that are communicated, followed and implemented
 - ✓ Routine testing to evaluate effectiveness of controls
 - ✓ A comprehensive security program is an integral part of the culture



Maturity

How has security changed over the last 10 years?

1. Hacking has gone pro
2. Everyone has been compromised
3. Breach detection tools have improved
4. Multi-factor authentication has proliferated
5. Encryption is the new default



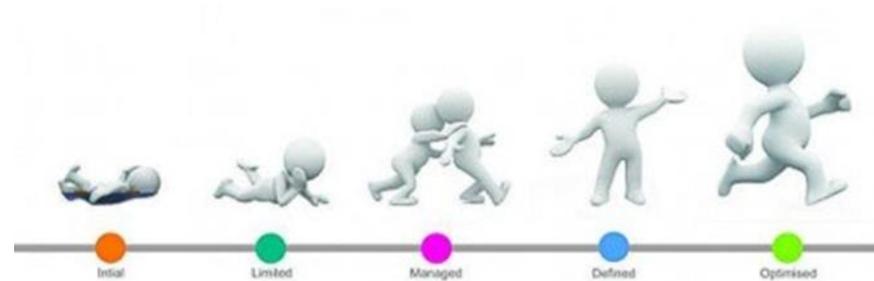
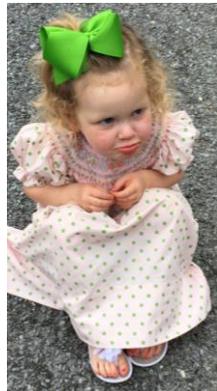
There are far more malicious attacks today than there were 10 years ago. "Improvements" in cyber crime have so far completely overwhelmed the advances in cyber security defense.

Roger A. Grimes, InfoWorld Aug. 2015

Maturity

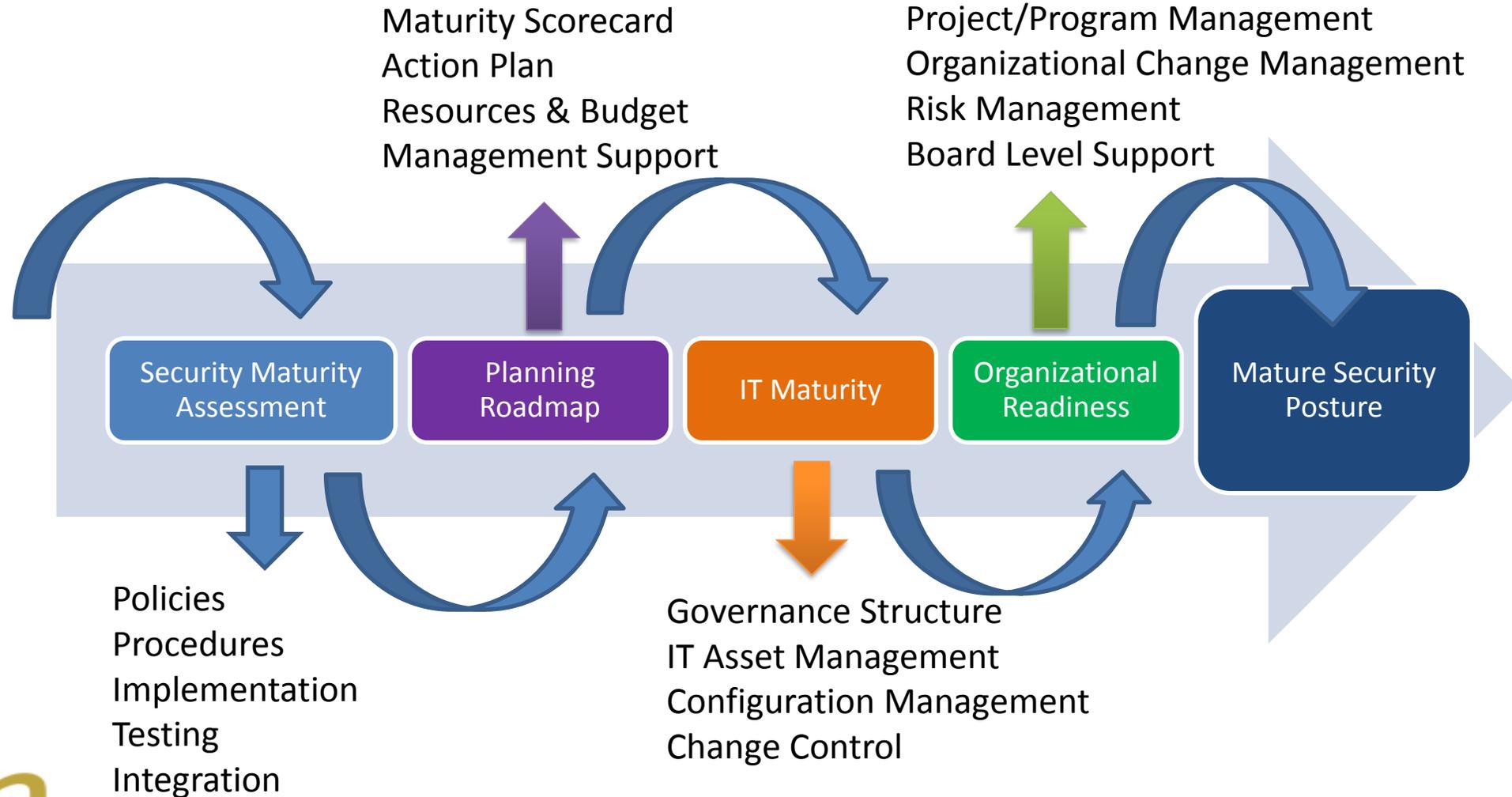
In a model

- Maturity is defined as reaching a desired state
- Maturity model then is an organized way of showing progression to a desired state
- Maturity models translate actions into goals that even *non-security* people can grasp.



Information Security

The Maturity Journey



PRISMA Introduction

Information Security Maturity Model

- Program Review for Information Security Management Assistance (NISTIR 7358)
- Incorporates guidelines contained in NIST SP 800-53 (SEC501)
- A methodology that is a means of employing a standardized approach to *review and measure* the information security posture of an information security program



Key Objectives

Leveraging PRISMA

- ✓ Identify program deficiencies and areas of risk
- ✓ Establish a program baseline to measure future improvement
- ✓ Validate completion of corrective actions or the “information security posture of the program”
- ✓ Assist in the identification and improvement of security/protection of confidential information, systems and interrelated components
- ✓ Support the implementation of more systematic, risk-based, and cost-effective information security frameworks and strategies.

9 PRISMA Topic Areas (TAs)

216 Sub-Topic Areas (STAs)

- Information Security Management and Culture (41)
- Information Security Planning (5)
- Security Awareness, Training, and Education (27)
- Budget and Resources (40)
- Lifecycle Management (21)
- Certification and Accreditation (6)
- Critical Infrastructure Protection (6)
- Incident and Emergency Response (30)
- Security Controls (40)



PRISMA Maturity Levels

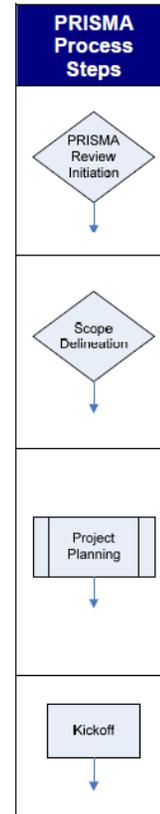
Five Levels of Cyber Security Program Maturity

- Maturity Level 1: Policies
 - ✓ *Shall or will language?*
- Maturity Level 2: Procedures
 - ✓ *Provided to implement policies?*
- Maturity Level 3: Implementation
 - ✓ *Communicated?*
- Maturity Level 4: Testing
 - ✓ *Tested to evaluate effectiveness?*
- Maturity Level 5: Integration
 - ✓ *Security as second nature?*

Independent Review

How does this work?

- Preparation
- Document Review
- Interviews
- Draft Report
- Comment and Clarify
- Finalize Report



Key Personnel Contact Request List	
Chief Information Officer (CIO)	Contract Managers
Chief Financial Officer (CFO)	Human Resource Managers
Chief Technology Officer (CTO)	Functional Area Managers
Senior Agency Information Security Officer (SAISO)	Program Managers
Inspector General (IG) Staff Personnel	Program Contracting Officers (CO)
Information Systems Security Managers (ISSMs)/ Officers (ISSOs)	Program Contracting Officer Technical Representative (COTR)
Designated Approval Authority (DAA)/ Authorizing Officials (AO)	System/ Network/ Database Administrators
Facilities Mgrs/ Physical Security Mgrs	IT Developers and/ or Integrators
Directors (IT, business areas, etc.)	End Users



TA	Management, Operational, and Technical Areas	Policy	Procedures	Implemented	Tested	Integrated
1	Information Security Management & Culture	0.63	0.60	0.30		
2	Information Security Planning	0.20	0.20			
3	Security Awareness, Training, and Education		0.65	0.37	0.31	
4	Budget and Resources		0.40	0.20		
5	Life Cycle Management					
6	Certification and Accreditation	0.80	0.30			
7	Critical Infrastructure Protection		0.60	0.30		
8	Incident and Emergency Response	0.80	0.50			
9	Security Controls	0.80	0.60	0.60		



Example

Interview Questions

PRISMA INDEX	TOPIC AREA (TA)	SUBTOPIC AREA (STA)	DOCUMENT CRITERIA	REFERENCE	Policy Question	Procedures Question	Implemented Question	Tested Question	Integrated Question
1.1.01	Information Security Management and Culture	IT Roles and Responsibilities	Are security roles defined, and are they assigned to individuals with their authority aligned to carry out their security responsibilities?	NIST SP 800-53; NIST SP 800-18	Does documented policy require security roles be defined, and are they assigned to individuals with their authority aligned to carry out their security responsibilities?	Are procedures documented requiring security roles be defined, and are they assigned to individuals with their authority aligned to carry out their security responsibilities?	Are security roles defined, and are they assigned to individuals with their authority aligned to carry out their security responsibilities?	Is periodic verification performed to ensure security roles are defined and assigned to individuals with their authority aligned to carry out their security responsibilities?	Is defining security roles and is assigning the roles to individuals with their authority aligned to carry out their security responsibilities accepted and standard business practices?
2.1.02	Information Security Planning	System Security Plans	Is each security plan periodically reviewed and adjusted to reflect current risks in order to remain effective?	NIST SP 800-53; NIST SP 800-18	To remain effective, does documented policy require each security plan to be periodically reviewed and adjusted to reflect current risks?	To remain effective, are procedures documented to periodically review and adjust each security plan to reflect current risks?	To remain effective, is each security plan periodically reviewed and adjusted to reflect current risks?	Are the security plans examined to determine if they are periodically reviewed and adjusted to reflect current risks?	Is a periodic review and adjustment of each security plan to reflect current risks and to maintain effectiveness a standard business practice?



Complete



Partially Complete



Not Complete

Example

Results Scorecard

TA	Management, Operational, and Technical Areas	Policy	Procedures	Implemented	Tested	Integrated
1	Information Security Management & Culture	0.63	0.60	0.30		
2	Information Security Planning	0.20	0.20			
3	Security Awareness, Training, and Education		0.65	0.37	0.31	
4	Budget and Resources		0.40	0.20		
5	Life Cycle Management					
6	Certification and Accreditation	0.80	0.30			
7	Critical Infrastructure Protection		0.60	0.30		
8	Incident and Emergency Response	0.80	0.50			
9	Security Controls	0.80	0.60	0.60		



Complete



Partially Complete



Not Complete



Getting to the next level

Maintain focus and visibility and answer tough questions

- How do our information security investments help further agency mission and goals?
- Are we more secure today than we were before?
- How do we compare to others in this regard?
- Are we secure enough?

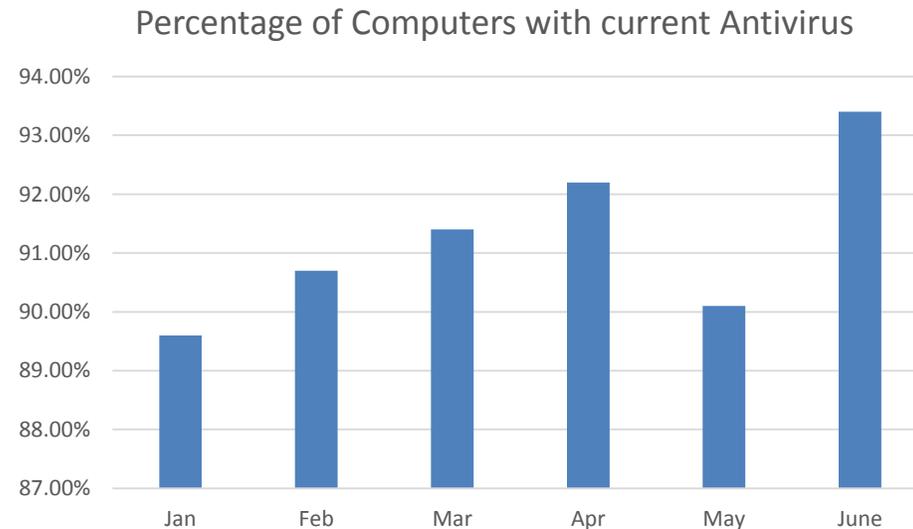
Metrics provide insight...



Measuring Performance

Metrics

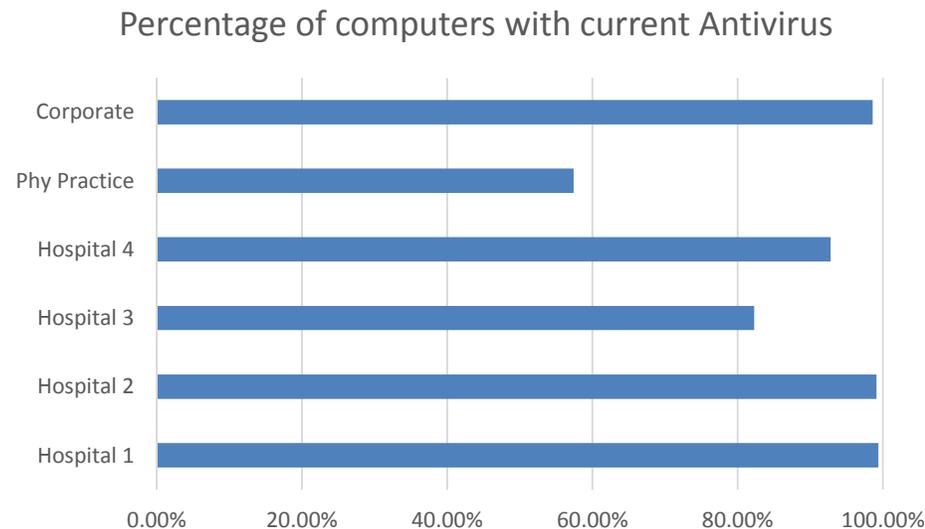
- An information security metric is an *ongoing* collection of measurements to assess security performance
- ***Absolute*** metrics are quantitative



Measuring Performance

Very important point about Metrics

- **Relative** metrics are metrics that involve quantitative measures that are “translated” or “mapped” to the priorities of leadership and are “actionable”.



Measuring Performance

Speaking the language of business and leadership

Absolute

- # of new accounts created during a specific time window
- Average length of time to create a new account
- # of infected endpoints during a specific time window
- # of brute force attempts during a specific time window

Relative

- Number of new access points into the network and systems during a specific time window
- Amount of time a new employee has to wait for access to systems to do their job
- Amount of sensitive data exfiltrated via infected endpoints during a specific time window
- Risk and exposure as a result of critical assets successfully compromised via brute force attacks during a specific time windows



In Summary

Final Thoughts

- 10 YEARS!
- Strong Cyber Security Posture is Critical
- Assess the maturity of your program
- PRISMA is one model that is publically available and mapped to NIST 800-53 (SEC 501)
- Keep the focus by measuring performance
- Speak the language that's meaningful

Comments and Discussion

Thank you!

Contact Information:

Cathie Brown

cbrown@impactmakers.org

Twitter @ctbrown86

