Measuring the Maturity of your Information Security Program. Impossible?

Presented by: Mark Carney, VP of Strategic Services
Information Security Program Maturity Models Agenda

- Definition of Mature
- Client Approaches to Governance, Risk, & Compliance (GRC)
- Purpose of Information Security Maturity Models
- Common Characteristics of Information Security Maturity Models
- Information Security Maturity Model – Marketplace Providers
- A closer look at FishNet Security’s Information Security Program Model (ISPM)
**Definition of MATURE**

1: based on slow careful consideration <a *mature* judgment>

2a *(1)* : having completed natural growth and development : *ripe*  
(2) : having undergone *maturation*

**b** : **having attained a final or desired state** <*mature wine*>  

**c** : having achieved a low but stable growth rate <paper is a *mature* industry>

**d** : of, relating to, or being an older adult : *elderly* <airline discounts for *mature* travelers>

3a : of or relating to a condition of full development  
**b** : characteristic of or suitable to a mature individual <*mature* outlook> <a show with *mature* content>

4: due for payment <a *mature* loan>
Information Security Program Maturity Models
Client Approaches to GRC

- Developing Security Governance Framework
- Security Metrics Program
- Measuring Information Security Program Maturity
- Unified Compliance Framework (UCF), or Controls-Based Framework Assessment/Gap Analysis
- ITGRC Solution Evaluation & Implementation
Information Security Program Maturity Models

Purpose

- Provide a foundation to build and develop an Information Security Program.
- Identify the gaps in your security program, evaluate its maturity, and better manage your security strategy.
- Ensure priority is placed on the most valued aspects of your security program.
- Articulate information security program’s value and progress to executives.
- Continually measure the maturity of one’s information security program against best practices or industry vertical peers.
Information Security Program Maturity Models

Common Characteristics

- Objective
- Prescriptive
- Modular
- Simple to Understand
- Leverage CMMI to Score Maturity Levels
- Strategy and Direction-setting Oriented
- Based off of Best Practices
- Reference Common Frameworks (ISO, NIST, COBIT 4.1, COBIT 5, PCI, and others)
Information Security Program Maturity Models
Marketplace Providers

- Large Public Accounting Firms
  - Big 4
- “Pure Play” Information Security Firms
  - FishNet Security
- Global IT Consulting Firms
  - Atos
- Security Software Manufacturers
  - Symantec
  - IBM
- Research Analysts
  - Forrester
The Forrester Information Security Maturity Model
Developed July 27th, 2010
Authors: Chris McClean, Khalid Kark, among nine others
Model consists of:
  - 4 Top-Level Domains (Oversight, People, Process, and Technology)
  - 25 Functions
  - 123 Components
Based on information security best practices (similar to CoBIT in terms of design)
Excel Spreadsheet based
Ability to collaborate and compare results with similar vertical companies through special Forrester services project
Cost $499
Symantec Security Program Assessment/Security Management Framework

- Developed: October 2007
- Point of Contact: John Hill
- Model consists of:
  - 3 Top-Level Domains (People “Strategic”, Process “Operational” and Technology “Tactical”)
  - 7 Core Areas
  - 42 Elements
- Based on information security best practices (ISO 27002, CoBIT, HIPAA, etc.)
- Delivery: Consulting/Specialized Service Offering
- Building Industry Vertical Repository
- Cost: $100k-$200k (4-6 weeks in duration)
Atos Enterprise Model Information Security

- Developed: June 2008
- Point of Contact: Unknown
- Model consists of:
  - 3 Top-Level Domains (Strategic, Tactical, and Operational)
  - 3 Core Areas (Policy, Architecture, and Controls)
- Based on information security best practices (ISO 27002, CoBIT, etc.)
- Delivery: Consulting
- Cost/Duration: Unknown
FishNet Security Information Security Program Model

- Developed: January 2012
- Authors: 12+ contributors
- Model consists of:
  - 3 Pillars (Governance & Policy, Risk, and Operations Management)
  - 23 Programs
  - 143 Strong Characteristics
- Based on information security best practices (ISO 27002:2005, CoBIT 4.1, CoBIT 5, NIST PS Series, NERC-CIP, and PCI)
- Delivery: Consulting
- Cost/Duration: $19,750/$31,500
Introduction to Information Security Program Model (ISPM)
Information Security Program Maturity Models
Closer Look @ ISPM
Information Security Program Model
Value vs. Priority Map – Current State

Information Security Program Model (ISPM):
Value vs. Priority Map

ISPM Programs
1. Governance Committee Leadership
2. Capital Planning & Investment
3. Policy Management
4. Strategic Business Alignment
5. Resource Management
6. Performance Measurement
7. Best Practices & Standards
8. Risk Assessment
9. Risk Management
10. Communication
11. Disaster Recovery
12. Malicious Activity Management
13. Security Awareness Training
14. Application Security
15. Asset Management
16. Physical & Environmental
17. Change Control
18. Engineering / Operations
19. Identity & Access Management
20. Vulnerability Scanning & Penetration Testing
21. Vendor Management
22. Incident Management

www.FishNetSecurity.com © 2012 FishNet Security. All rights reserved.
### Initiative: Develop an effective logging and monitoring program

#### Initiative Summary:

Current Maturity (CMMI): **2.25**  
ABC Inc. will undertake an initiative to develop an enterprise wide approach to the collection and management of log files for key systems within the ABC, Inc. computing environment. This will include...

- **Sub-Initiatives**
  - Develop a log management framework
  - Develop business, staffing and...
  - Conduct a software monitoring / management tool inventory

#### Result of Completed Initiative:

- **Future Maturity (CMMI): 4.25**  
  - ABC Inc. will have the ability to take a proactive approach to addressing network and access issues. Compliance mandates will be addressed...

#### Funding/Resource Requirements:

- **Internal Labor**
  - Yes – SME input for technical and business requirements. Industry average: Minimum 9 resources to manage SNOC
  
- **External Labor**
  - Yes - Solution specific expertise

- **Other Costs**
  - Capital – Yes: Product
  - Expense – Yes: Ongoing maintenance / support, staffing, and product owner training

#### Risks:

- Impact to business operations due to a data breach or service outage
- ABC Company could be in violation of compliance mandates
- Increase time to identify and resolve network and access issues
- Inability to answer the ‘why’ question during a post incident review

#### Key Tasks/Owners:

- Identify compliance mandate requirements
- Conduct staffing feasibility assessment
- Develop business and technical solution requirements
- Develop...
- Gain support...
- Conduct a...
- Determine the...
- Roll out the...

#### Related Initiatives:

- None

#### Executive Sponsor:

- CIO

#### Project Manager:

- IT Delivery Manager

#### Key Staff Members:

- IT, Security, Audit

#### Key Skillsets Required:

- Information Security SMEs, product SME(s)

- Executive stakeholder involvement and buy in (CEO, CIO, CISO)
- Resource and expertise availability
- Business unit buy-in

#### Complexity:

- High

#### Resources Required:

- Executive stakeholder involvement and buy in (CEO, CIO, CISO)
- Resource and expertise availability
- Business unit buy-in

End of Q4 2013

**Importance:** HIGH
Information Security Program Model
Strategic Roadmap

- Develop Logging & Monitoring Program
- BYOD Strategy
- Migrate to a Unified Compliance Approach
- Security Technology Prioritization Roadmap
- Develop Metrics Program
- Security Awareness & Training Program
- Integrate Security Initiatives with Business Strategies
- Develop RFI for GRC Solution
- ISPM Tollgate
- Store Locations Information Security Assessments
- Network Segmentation Review
- ISPM Tollgate
- Conduct a Data Security Analysis

24-Month View

Q4 2012 - 2013 - 2014 Q1 Q2 Q3 Q4 Q1
Information Security Program Model
Thank You

Mark Carney
CISSP, CRISC, C|CISO, PCI-QSA, NSA-IAM, MBA
Vice President, Strategic Services
Mark.Carney@FishNetSecurity.com
Twitter: MarkRCarney
LinkedIn: www.linkedin.com/pub/mark-carney/0/537/72a

Fishnetsecurity.com 6Labs.net 888.732.9406

facebook.com/fishnetsecurity
twitter.com/fishnetsecurity

http://www.fishnetsecurity.com/6labs/blog/can-you-really-measure-maturity-your-information-security-program