Secure360

Measuring the Maturity of your Information Security Program Impossible?

Presented by: Mark Carney, VP of Strategic Services
HOW DO YOU KNOW IF YOU ARE GETTING THE MOST OUT OF YOUR LIFE?
Information Security Program Maturity Models
Parallels Between Life and Information Security

- Complex
- Dynamic
- Unpredictable
- Limited Amount of Time
- Limited Amount of Money
- The Decisions You Make are Critical
Information Security Program Maturity Models
Managing Life and Information Security Programs

- **Build Foundation**
  - Create a Mission Statement and Vision
  - Pillars/Principles
- **Periodically Evaluate**
  - Review strengths and weaknesses
- **Develop Roadmap**
  - Goals and Priorities
- **Be Prepared**
  - Leave a legacy
My Life Model (MLM)

- Spiritual
- Intellectual
- Physical
My Life Priorities

1. Spiritual Beliefs
2. Family
3. Friends
4. Health (Physical & Financial)
5. Work
Information Security Program Maturity Models

How InfoSec Models Help?

- Provides a foundation
- Identify the gaps, evaluate its maturity, and better manage
- Ensures priority is placed on the most valued aspects
- Articulate program’s value and progress
- Continually measures the program against best practices and/or industry vertical peers.
- Sets Direction and Develops Roadmap
Definition of Mature

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*

2b: having attained a final or desired state, *mature wine*

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*
Client Approaches to GRC

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

- Large Public Accounting Firms
- “Pure Play” Information Security Firms
- Global IT Consulting Firms
- Security Software Manufactures
- Research Analysts
- Federal Agencies
Forrester’s Information Security Maturity Model

- 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 InfoSec best practices
  - Similar to CoBIT in terms of design
- Excel Spreadsheet based
- Vertical Comparisons
- Cost $499
Symantec’s Security Program Assessment

- 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
    - Organization, Strategy, Operations, Data, Application, Network & System, and BCM
  - 42 Elements
- Based on information security best practices (ISO 27002, CoBIT, HIPAA, etc.)
- Delivery: Consulting/Specialized Service Offering
- Building Industry Vertical Repository
- Cost: 4-8 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 InfoSec best practices (ISO 27002, CoBIT, and others)
- Delivery: Consulting
- Cost/Duration: Unknown
Information Security Program Maturity Models

ES-C2M2

- Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
- Developed: September 2011
- Authors: 85 contributors
- Model consists of:
  - 10 Domains (Risk, Asset, Access, Threat, Situation, Sharing, Response, Dependencies, Workforce, and Cyber)
- Maturity Ranking: CCMI
- Delivery: Self Evaluation
- Cost/Duration: 1-Day
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
  - 157 Strong Characteristics
- Based on infosec best practices
  - (ISO 27002:2005, CoBIT 4.1, CoBIT 5, NIST PS Series, NERC-CIP, and PCI)
- Delivery: Workshop/Consulting
- Duration: 2-Days/Toll-Gates
Information Security Program Maturity Models

A Closer Look @ ISPM
Results of an Information Security Maturity Model?
Information Security Program Model

Evaluate Current vs. Desired State

Overall ISPM Comprehensive CMMI Score 2.75

Information Security Program Model (ISPM)

Pillars

Governance & Policy 3
- Governance Committee Leadership 4
- Strategic Business Alignment 3.25
- Capital Planning & Investment 3.75
- Policy Management 2.75
- Performance Measurement 1
- Best Practices & Standards 2.75

Risk 2
- Risk Assessment 2
- Risk Management 2

Operations Management 3
- Incident Management 2.5
- Communication 2.75
- Disaster Recovery 4.25
- Malicious Activity Management 1.75
- Security Awareness Training 3.5
- Application Security 2.75
- Asset Management 3.75
- Physical & Environmental 4
- Change Control 4
- Engineering/Operations 2.25
- Vendor Management 2.5
- Vulnerability Scanning & Penetration Testing 2.75

Corporate | Compliance (PCI, ISO27001, GLBA, HIPAA, SSAE16, SOX)

Risk Metrics & Key Program Performance Indicators (KPPIs)

Executive / Business Leadership
External Audit
Internal Audit / General Council

© 2013 FishNet Security Inc. All rights reserved.
**Initiative:** Develop an effective logging and monitoring program

**Target Completion:** End of Q4 2013

**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

**Current Maturity (CMMI):** 2.25

**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...

**Result of Completed Initiative**

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

**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

**Executive Sponsor**

- CIO

**Key Staff Members**

- IT Delivery Manager
- IT, Security, Audit

**Key Skillsets Required**

- Information Security SMEs, product SME(s)

**Complexity**

- High

**Resources Required**

- Executive stakeholder involvement and buy in (CEO, CIO, CISO)
- Resource and expertise availability
- Business unit buy-in
# Information Security Program Model

## Targeted Roadmap

<table>
<thead>
<tr>
<th>Ref#</th>
<th>Recommendation</th>
<th>Program</th>
<th>Priority</th>
<th>Initiative Start</th>
<th>Resource</th>
<th>Product Component</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST-01</td>
<td>Develop and effective Logging and Monitoring program</td>
<td>Operations Management</td>
<td>High</td>
<td>Q4 2012</td>
<td>Internal</td>
<td>Yes</td>
<td>$</td>
</tr>
<tr>
<td>ST-02</td>
<td>Build a BYOD strategy and plan</td>
<td>Strategic Business Alignment</td>
<td>High</td>
<td>Q4 2012</td>
<td>Blended</td>
<td>Yes</td>
<td>$$</td>
</tr>
<tr>
<td>ST-03</td>
<td>Migrate to a unified compliance approach for audit and assessment activities</td>
<td>Risk Management</td>
<td>High</td>
<td>Q4 2012</td>
<td>Blended</td>
<td>Yes</td>
<td>$$$</td>
</tr>
<tr>
<td>ST-04</td>
<td>Develop the security...</td>
<td>Communications</td>
<td>High</td>
<td>Q1 2013</td>
<td>Internal</td>
<td>No</td>
<td>$$$$</td>
</tr>
<tr>
<td>ST-05</td>
<td>Conduct a data security...associated with the data types used throughout ABC Inc.</td>
<td>Communications</td>
<td>Medium</td>
<td>Q1 2014</td>
<td>Blended</td>
<td>Possible</td>
<td>$$</td>
</tr>
<tr>
<td>ST-07</td>
<td>Define business requirements...for a enterprise wide GRC solution</td>
<td>Policy Management / Risk Management</td>
<td>Medium</td>
<td>Q2 2013</td>
<td>Internal</td>
<td>Yes</td>
<td>$$</td>
</tr>
</tbody>
</table>
Information Security Program Maturity Models

Closing Questions

DO YOU HAVE A STRONG FOUNDATION?

DO YOU KNOW YOUR TOP PRIORITIES?

DO YOU HAVE A ROADMAP?
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