Measuring Cybersecurity Readiness: The Cybersecurity Maturity Model

NCHICA Cybersecurity Thought Leader Forum

Richard Roberts, CISO & Director of Technology Strategy
What is a Cybersecurity Maturity Model?

A cybersecurity maturity model allows an organization to compare cybersecurity people, processes and technology against a predetermined set of external benchmarks. A maturity model also helps an organization answer the ”how do we know?” questions.

• How do we know our current state of affairs?
• How do we know where we need to go?
• How do we know what we are good at?
• How do we know if we are improving?
• How do we know if the processes we are using are working well?
• How do we know how we compare relative to our peers?

The last question is key to our discussion today. “How do we compare to our peers?”
Why Does It Matter What Everyone Else Is Doing?

Many organizations are using compliance as their benchmark. The problem with this is compliance does not equal security. An established Healthcare Maturity Model allows for:

• A benchmark for organizations to compare themselves to
• A benchmark for organization to compare themselves to their peers
• Insight into the current state of the Healthcare Industry as a whole
  • by reporting relative maturity levels at the local, state and federal levels
  • This could a tool to help open the door for outside funding (think Meaningful Use)
• Build consensus both internally and throughout the industry
  • by communicating and engaging with the organization to agree a shared vision of how information security can support strategic goals
  • by facilitating business-based discussions with decision-makers.
Why Does It Matter What Everyone Else Is Doing?

• Prioritize Investment
  • by using the maturity model for planning and prioritizing specific actions to achieve strategic goals
  • by supporting normal business planning and focusing on areas of value to the organization

• Demonstrate progress
  • by using maturity as an informative and consistent metric to measure and compare progress across different areas of information on security or business units
  • by allowing the CISO to answer senior management questions about how the organizations compares to its peers and competitors

• Move the industry forward
  • by working together we can be stronger and more effective and than working as individuals
  • by following examples already set in other industries
HIPAA Security Rule – Overview, Compliance is not Enough

- The Privacy Rule and Security Rule Compared: The Privacy Rule sets the standards for, among other things, who may have access to PHI, while the Security Rule sets the standards for ensuring that only those who should have access to EPHI will actually have access. (Note: Implementation specifications in the Security Rule are either “Required” or “Addressable”).
  - See 45 C.F.R. § 164.306(d).
  - (c)(1) Standard specification: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI).
  - (2) Implementation specification: safeguards.
  - (i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.
  - (ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.
Maturity Model Examples

<table>
<thead>
<tr>
<th>Category</th>
<th>Basic Organizations</th>
<th>Progressing Organizations</th>
<th>Advanced Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Philosophy</td>
<td>Cybersecurity is a &quot;necessary evil.&quot;</td>
<td>Cybersecurity must be more integrated into the business.</td>
<td>Cybersecurity is part of the culture.</td>
</tr>
<tr>
<td>People</td>
<td>CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.</td>
<td>CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.</td>
<td>CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.</td>
</tr>
<tr>
<td>Process</td>
<td>Informal and ad-hoc. Subservient to IT.</td>
<td>Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.</td>
<td>Documented and formal with an eye toward more scale and automation.</td>
</tr>
</tbody>
</table>


InfoSec Maturity Model

- **Reactive**
  - Blocking & Tackling
    - Lack of Executive support
    - Underfunded
    - Understaffed
    - Lack of metrics for reporting
    - Set up for failure

- **Compliance Driven**
  - Control-based security approach
  - Align to mandatory regulations
    - EU/PII Data protection
    - FFIEC
    - HIPAA
    - ISO 2700x
    - PCI
    - NCUA

- **Risk-Based Approach**
  - Multi-layered security and risk-based approach
  - Using behavior analytics and evaluating new technologies frequently
  - Linking events across multiple disciplines

Source: Blue Lava Consulting

Maturity Models

Source: Blue Lava Consulting
## Basic Maturity Matrix

<table>
<thead>
<tr>
<th>Category</th>
<th>Basic Organizations</th>
<th>Progressing Organizations</th>
<th>Advanced Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Philosophy</td>
<td>Cybersecurity is a “necessary evil.”</td>
<td>Cybersecurity must be more integrated into the business.</td>
<td>Cybersecurity is part of the culture.</td>
</tr>
<tr>
<td>People</td>
<td>CISO reports to IT. Small security team with minimal skills. High burnout rate and</td>
<td>CISO reports to COO or other non-IT manager. Larger security team with</td>
<td>CISO reports to CEO and is active with the board. CISO considered a business executive.</td>
</tr>
<tr>
<td></td>
<td>turnover.</td>
<td>some autonomy from IT. Remain overworked, understaffed, and under-skilled.</td>
<td>Large, well-organized staff with good work environment. Skills and staff problems persist</td>
</tr>
<tr>
<td></td>
<td>Informal and ad-hoc. Subservient to IT.</td>
<td>Better coordination with IT but processes remain informal, manual, and dependent upon</td>
<td>due to the global cybersecurity skills shortage.</td>
</tr>
<tr>
<td>Process</td>
<td></td>
<td>individual contributors.</td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td>Elementary security technologies with simple configurations. Decentralized security</td>
<td>More advanced use of security technologies and adoption of new tools for incident detection</td>
<td>Building an enterprise security technology architecture. Focus on incident prevention,</td>
</tr>
<tr>
<td></td>
<td>organization with limited coordination across functions. Focus on prevention and</td>
<td>and security analytics.</td>
<td>detection, and response. Adding elements of identity management and data security to</td>
</tr>
<tr>
<td></td>
<td>regulatory compliance.</td>
<td></td>
<td>deal with cloud and mobile computing security.</td>
</tr>
</tbody>
</table>

*Source: Enterprise Strategy Group, 2014.*
EXISTING CYBERSECURITY MATURITY MODELS
CMMI Capability Maturity Model

Characteristics of the Maturity Levels

- **Level 1 (Initial)**: Processes unpredictable, poorly controlled and reactive
- **Level 2 (Managed)**: Processes characterized for projects and is often reactive
- **Level 3 (Defined)**: Processes characterized for the organization and is proactive
- **Level 4 (Quantitatively Managed)**: Processes measured and controlled
- **Level 5 (Optimizing)**: Focus on process improvement

Focus on process improvement
C2M2

- **C2M2** - A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. Model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline. A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement. Also, when a model is widely used in a particular industry (and assessment results are shared), organizations can benchmark their performance against other organizations. *An industry can determine how well it is performing overall by examining the capability of its member organizations.*

1. Source: US Dept. of Energy
An ISECOM standard, ISM^3 defines maturity in terms of ISM processes and three broad levels of management responsibility in terms of four models:

- Information Security Management Model: Provides a framework for identifying the key processes in an ISM system and evaluating their maturity.

- Organizational Model: Provides a responsibilities-based view of an organization;

- Information System Model: Provides a way of describing the main components and Properties of information systems;

- Security in Context Model: allows an organization to prepare its own definition of security suited to the environment and mission of the organization
### Gartner IAM Maturity Model

<table>
<thead>
<tr>
<th>IAM Program Maturity Level</th>
<th>Initial</th>
<th>Developing</th>
<th>Defined</th>
<th>Managed</th>
<th>Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Governance</strong></td>
<td>Ad hoc, informal</td>
<td>Subsumed within InfoSec (and InfoSec governance structures)</td>
<td>IAM governance structure defined and accepted</td>
<td>IAM governance structure fulfilled and refined</td>
<td>IAM governance optimization</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Informal, basic roles, responsibilities decentralized</td>
<td>Technical projects sponsored by BUs and CISO; informal inventory of IAM skills</td>
<td>IAM PMO established, IAM roles and training needs defined</td>
<td>IAM PMO active, RACI matrix defined; proactive skill development</td>
<td>Optimal integration with business; skills optimized</td>
</tr>
<tr>
<td><strong>Vision and Strategy</strong></td>
<td>Conceptual awareness at best</td>
<td>Certain business drivers identified; tactical priorities set</td>
<td>Business-aligned vision defined; strategic priorities set</td>
<td>IAM vision and strategy continually reviewed to track business strategy</td>
<td>Periodic optimization of vision and strategy</td>
</tr>
<tr>
<td><strong>Processes</strong></td>
<td>Ad hoc, informal</td>
<td>Semiformal BU-specific and target-specific processes</td>
<td>Formal processes defined, consistent across BUs and target systems</td>
<td>Formal processes integrated and refined; aligned with business processes</td>
<td>Process optimization</td>
</tr>
<tr>
<td><strong>Architecture and Infrastructure Design</strong></td>
<td>Possible use of target-specific productivity tools</td>
<td>Disjoint technical projects; technology redundancy likely</td>
<td>Discrete IAM architecture defined; rationalization and consolidation in hand</td>
<td>IAM architecture refined and aligned with EA</td>
<td>IAM architecture embedded within EA; optimization</td>
</tr>
<tr>
<td><strong>Business Value</strong></td>
<td>None measurable</td>
<td>Tactical efficiency and (maybe) effectiveness improvements; low direct value</td>
<td>Sustained, quantifiable improvements tied to GRC imperative; moderate direct value</td>
<td>Sustained, quantifiable contribution to all key business imperatives; high direct value</td>
<td>Business value optimization; transformational direct value</td>
</tr>
</tbody>
</table>

**Legacy Program Maturity Level** | **Blissful Ignorance** | **Awareness** | **Corrective** | **Operational Excellence**

BU: business unit; IAM: identity and access management; PMO: program management office; EA: enterprise architecture; RACI: responsible-accountable-consulted-informed; GRC: governance, risk and compliance
Gartner Security Maturity Model

Level of Program Maturity

0: Blissful Ignorance
1: Awareness
2: Corrective
3: Operations Excellence

- Review Status Quo
- Design Architecture
- Develop New Policy Set
- Conclude Catch-Up Projects

- Process Formalization
- Initiate Strategic Program
- 10%
- 5%

- Continuous Process Improvement
- Track Technology and Business Change

- Composite Risk Position
- (Re-)Establish Security Team
- 35%
- 30%

5/15/2012 DIR Information Security Forum
Blue-Lava.net InfoSec Security Model

InfoSec Maturity Model

Reactive

Blocking & Tackling

- Lack of Executive support
- Underfunded
- Understaffed
- Lack of metrics for reporting
- Set up for failure

Compliance Driven

- Control-based security approach
- Align to mandatory regulations
  - EU/PII Data protection
  - FFIEC
  - HIPAA
  - ISO 2700x
  - PCI
  - NCUA

Proactive

Risk-Based Approach

- Multi-layered security and risk-based approach
- Using behavior analytics and evaluating new technologies frequently
- Linking events across multiple disciplines

Source: Blue Lava
Blue-Lava.net InfoSec Security Model

- **Level 1** – Information Security processes are unorganized, and may be unstructured. Success is likely to depend on individual efforts and is not considered to be repeatable or scalable. This is because processes would not be sufficiently defined and documented to allow them to be replicated.

- **Level 2** – Information Security efforts are at a repeatable level where basic project management techniques are established and successes can be repeated. This is due to processes being established, defined, and documented.

- **Level 3** – Information Security efforts have greater attention to documentation, standardization, and maintenance support.

- **Level 4** – At this level, an organization monitors and controls its own Information Security processes through data collection and analysis.

- **Level 5** – This is an optimizing level where Information Security processes are constantly being improved through monitoring feedback from existing processes and introducing new processes to better serve the organization’s particular needs.
# Blue-Lava.net InfoSec Security Model

## Maturity Models

<table>
<thead>
<tr>
<th>Business Unit</th>
<th>Awareness and Training</th>
<th>Compliance and IT Audit</th>
<th>Emerging IT/Threats</th>
<th>Incident Response (IR)</th>
<th>Operations and Support</th>
<th>SDLC</th>
<th>PMO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Information Security Maturity Model (ISMM)
Gartner ITScore

Gartner's ITScore Maturity Levels for Information Security

**Level 1: Initial**
- Ad hoc activities
- Initial executive awareness
- IT-centric approach initiated

**Level 2: Developing**
- CISO appointed
- User awareness outreach
- Formal program initiated

**Level 3: Defined**
- Policies and processes defined
- Security organization defined
- Improving user awareness
- Security organization working well

**Level 4: Managed**
- Governance body established
- Info-centric approach
- Effective metrics
- Refinement for changes in business, technology, compliance and economic environments

**Level 5: Optimizing**
- Information owners accountable
- Risk-aware culture

© 2015 The SANS™ Institute – www.sans.org
DOES HEALTHCARE NEED A CYBERSECURITY MATURITY MODEL?
Is there value in a nationally recognized standard for a healthcare specific CSMM?
  - What would make a healthcare model unique?
  - Many existing models, why one more?
  - What organization would be best for publishing a healthcare specific CSMM standard?

Which industries should healthcare look to as a model to measure its maturity against?
  - Is there a “gold standard” e.g. Finance, DOD, Energy that healthcare should be measuring itself against?
  - Are there lessons to be learned from failures in other industries such as insurance and retail?

What steps should industry and government be taking to facilitate a move towards national standards?
  - Is the healthcare industry too fragmented to come together around a standard?
  - Will the cybersecurity insurance industry support a healthcare CSMM?
  - Who will be the certifying body?
Does Healthcare Need A Cybersecurity Maturity Model?

• What will make this model a useful, real-world tool?
  – What level of detail would the model require?
  – What standards to incorporate?
  – How closely would it follow existing standards such as NIST or HITRUST
  – Would it require a large data set to benchmark against to be useful?

• How would using this tool help organizations drive investment in cybersecurity and help organizations build cybersecurity strategies and roadmaps?
  – Would a healthcare specific CSMM actually drive investment?
  – Could a healthcare specific CSMM provide a roadmap for cybersecurity investment?

• What are the risks in measuring an organizations cybersecurity and sharing information across organizations?
  – Would an organization that is at a low maturity level be putting itself at risk if the information around its security maturity level becomes known?
  – Will organizations see other risks (competitive, otherwise) in sharing information?
  – Is there a risk in this becoming a government rating or mandate beyond existing HIPAA rules?
Does Healthcare Need A Cybersecurity Maturity Model?

- What are the risks in measuring an organizations cybersecurity and sharing information across organizations?
  - Would an organization that is at a low maturity level be putting itself at risk if the information around its security maturity level becomes known?
  - Will organizations see other risks (competitive, otherwise) in sharing information?
  - Is there a risk in this becoming a government rating or mandate beyond existing HIPAA rules?
THANK YOU