CERT PODCAST SERIES: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Why Use Maturity Models to Improve Cybersecurity: Key Concepts, Principles, and Definitions

Key Message: Maturity models are providing measurable value in improving an organization's cybersecurity capabilities.

Executive Summary

In recent years, rapid evolutions have occurred in technology and its application in most market sectors, leading to the introduction of many new systems, business processes, markets, and enterprise integration approaches. How do you manage the interactions of systems and processes that are continually evolving? Just as important, how can you tell if you are doing a good job of managing these changes, as well as monitoring your progress on an ongoing basis? And how do poor processes impact interoperability, safety, reliability, efficiency, and effectiveness? Maturity models can help you answer these questions by providing a benchmark to use when assessing how a set of security practices has evolved. [1]

In this podcast, Rich Caralli, the technical director of CERT's Cyber Enterprise and Workforce Management Directorate, discusses maturity models and how they are being used to improve cybersecurity. He describes their key concepts, definitions, and principles and how these can and have been applied to a wide range of disciplines and market sectors.

This podcast is based on two white papers that Rich and his co-authors have developed, titled "Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability" [1] and "Discerning the Intent of Maturity Models from Characterizations of Security Posture." [2]

PART 1: WHAT ARE MATURITY MODELS AND WHY ARE THEY USEFUL?

Why Discuss Maturity Models Now?

Maturity models have been around for a long time, applied to software and system engineering. A whole new community is starting to consider their benefits and advantages, particularly for cybersecurity in the public and private sectors.

The CERT Resilience Management Model has been a work in progress for 10 years. A number of organizations have used it successfully and developed derivatives from it that are gaining traction today including:

- U.S. Department of Homeland Security Cyber Resilience Review (CRR), which helps owners and operators of critical infrastructures evaluate their resilience practices
- U.S. Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which helps electric utilities and grid operators assess their cybersecurity capabilities

In CERT's collaboration with the GridWise Architecture Council, we noticed the uptick in interest in maturity models. However:

- Not all models are created equal.
- Many purport to be capability maturity models (CMM) but don't have the requisite architecture or characteristics of one.
- If not done properly, maturity models can have a detrimental effect for those using them.

If done properly, such models can be useful tools for transforming organizations and measuring effectiveness. This is much more desirable than measuring compliance and implementation.

Are Models High Overhead?

Many think that maturity models are labor and resource intensive and require a significant organizational commitment. In CERT's experience, models can be scoped and tailored to address a specific problem.

This makes the barrier to use much lower and the ability to use a model over time much greater.

Definitions

A maturity model

- is a set of characteristics, attribute, indicators, or patterns that represent progression and achievement in a particular domain or discipline. It is, essentially, a progression of processes, practices, and technologies.
- creates a benchmark against which an organnzation can assess their current level of achievement or capability
- reflects a community's experience and knowledge
- provides a common language and a shared vision
- defines what improvement means and a roadmap for achieving it
- provides a framework to prioritize next steps and actions
- provides a reference model and dictionary that defines terms and relationships
- provides goals and practices – a body of knowledge – from which you can derive useful and practical applications of the model

---

PART 2: STRUCTURE AND COMPONENTS

Components of a Maturity Model

Maturity models, by definition, have:

- levels, often referred to as maturity levels or capability levels. Names of levels reflect that characteristics that exist at that level (for example, adhoc, managed, defined, quantitatively managed, optimized)
- domains or process areas, which are groupings of related practices, for example, incident management
- attributes, which occur at the intersection of a domain and a maturity level, such as the use of a specific technology
- an appraisal process, used to evaluate an organization's capability against the model
- an improvement roadmap method (plan/do/check/act

Maturity Level Transitions and Collecting Evidence of Effectiveness

One of the biggest challenges for maturity models is defining the transition between maturity levels. Effective models have measurable transitions that are based on empirical data that has been validated through use.

Most maturity models start with a community of subject matter experts and their anecdotal experiences. Validating a useful transition from one practice to a more mature practice includes demonstrating that the more mature practice is indeed more effective and produces a better (in this case, more secure) result.

Building a model based on a community's best experiences is useful. Such models can "simmer" as the community learns about what works well and what doesn't and begins to collect evidence of practice effectiveness – updating the model over time.

PART 3: THREE TYPES OF MODELS – PROGRESSION, CAPABILITY, HYBRID

Progression Models

A progression model describes a scaling of characteristics, indicators, attributes, or patterns. An accounting example is:

- level 1: pencil and paper
- level 2: abacus
- level 3: calculator
- level 4: computer

A progression model does not measure capability or process maturity; it typically presents a progression of practices or technologies from "least mature" to "more mature" implementation. An authentication example is:

- simple passwords
- strong passwords
- passwords changes every 60 days
- two-factor authentication
- three-factor authentication

Capability Models

A capability model measures organizational capability as a set of characteristics, indicators, attributes, or patterns, which are typically expressed as processes. Using a capability model is often described as model-based process improvement.

Capability models reflect the maturity of the culture and the degree to which capabilities are institutionalized in the culture – the way the organization does business in normal times and under times of stress.

A capability model description of the authentication example above would include management, planning, measurement, and other activities that makes a process or practice "sticky." In this type of model, a practice still performs as intended and is robust in the presence of disruption.

In such a model, the dimension that is being measured is organizational capability, the maturity of the culture, and the extent to which capabilities are embedded. The transitions between maturity levels describes states of organizational maturity.

This approach allows an organization not only to measure whether or not they are performing practices but also whether or not they are doing it well.

Hybrid Models

A hybrid model is intended to combine the best of a progression model and the best of a capability model. This type of model reflects a progression from rudimentary practices to more sophisticated practices. In addition, the transition between maturity levels reflects the extent to which the practice is institutionalized, i.e., part of the organization's way of doing business.

This allows the hybrid model to be used to measure progression and maturity at the same time.

One example is ES-C2M2. The hybrid approach is reflected in the definition of the Maturity Indicator Levels (MIL) as follows:

- MIL 1: practices performed in an ad hoc manner
- MIL 2: practices documented; stakeholders identified; resources provided; standards identified

- MIL 3: practices guided by policy that are reviewed on a regular basis; responsibilities assigned; people performing practices are highly skilled

In this approach, not only do practices mature from MIL 1 to MIL 2 to MIL 3 but the "stickiness" factors are also more mature, moving from ad hoc to documented and planned.

Feedback on this approach indicates that combining practice maturity and capability maturity aids in conducting assessments and implementing improvements. This approach helps deal with the complexity of maturity concepts by making these more embedded.

Users report that this approach is more agile, easier to understand, and easier to apply.

Future Plans

Future plans include new reports and papers on the following topics:

- Maturity indicator levels and scales, for use with hybrid models
- A review of maturity models in use today, how they are being managed, and the community benefits including transformation

---

Resources

[1] Caralli, Richard; Knight, Mark; Montgomery, Austin. "Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability." Carnegie Mellon University: Software Engineering Institute, November 2012 (pending publication).

[2] Caralli, Richard. "Discerning the Intent of Maturity Models from Characterizations of Security Posture." Carnegie Mellon University: Software Engineering Institute, January 2012 (pending publication).

CERT Resilience Management Model website.

Electric Subsector Cybersecurity Capability Maturity Model website.

CERT Podcast: Adapting to Changing Risk Environments: Operational Resilience, May 2007.

CERT Podcast: How Resilience Is My Organization, December 2010.