APPLICATION OF MATURITY MODELS FOR EVALUATING CYBERSECURITY PROGRAMS AT NUCLEAR AND RADIOLOGICAL FACILITIES

C. GLANTZ
S. CLEMENTS
P. PEDERSON
G. LANDINE
R. GOYCHAYEV
Pacific Northwest National Laboratory
Richland, Washington USA
Email: cliff.glantz@pnnl.gov

C. NICKERSON
Idaho National Laboratory
Idaho Falls, Idaho USA

G. WHITE
Lawrence Livermore National Laboratory
Livermore, California USA

L. DAWSON
Sandia National Laboratories,
Albuquerque, New Mexico USA

Abstract

Maturity models can be used to provide government agencies, industry associations, and organizations operating nuclear facilities with the ability to quickly evaluate the maturity of their cybersecurity programs and identify areas to prioritize for improvement. The Cybersecurity Capability Maturity Model (C2M2) was developed by the U.S. Department of Energy to allow organizations in the energy sector to evaluate the programmatic capabilities of their cybersecurity programs in a consistent manner, communicate programmatic maturity information, prioritize cybersecurity investments in targeted areas of concern, and track how the maturity of their cybersecurity program evolves over time. The C2M2 is designed for use by any critical infrastructure organization regardless of ownership, structure, or size. The C2M2 can be easily fine-tuned to assess the maturity of nuclear cybersecurity programs and their application at individual facilities. Built on a foundation of existing cybersecurity standards, frameworks, programs, and initiatives, the model features 10 security domains. Performance in each security domain is characterized using a structured set of cybersecurity practices that represent activities an organization can perform to improve cybersecurity in their domain. Each practice can be quickly evaluated as being either fully, largely, partially, or not implemented. Once practices are evaluated for each security domain, the model defines four maturity indicator levels that apply independently to each domain in the model. To earn a maturity level in a given domain, an organization must adequately perform all the practices for that maturity level and its predecessor level(s). A small assessment team can conduct a C2M2 assessment in a single day. A screening version of the C2M2 allows an initial look at the maturity of nuclear cybersecurity programs that could be completed in under an hour.

1. INTRODUCTION

Laws and regulations in many countries set minimum requirements for cybersecurity and may or not fully incorporate good or best cybersecurity practices for protecting the confidentiality, integrity, and availability of digital systems and information at nuclear facilities. This is especially true in countries where laws and regulations are not up to date with the current cyber threat environment. Government regulators, industry associations, and the organizations operating nuclear facilities could benefit from a quick and inexpensive way to judge the maturity of the programmatic aspects of their nuclear cybersecurity programs and identify programmatic areas that might benefit from increased attention. A maturity model provides a way to gauge current performance, select performance targets, and prioritize programmatic activities that provide the most cost-effective way of enhancing nuclear cybersecurity programs. To address this issue for the overall energy sector (including the electricity, oil, and natural gas subsectors), as well as other critical infrastructure sectors, the U.S. Department of Energy developed the Cybersecurity Capability Maturity Model (C2M2) in partnership with the U.S. Department of Homeland Security, private- and public-sector experts, and representatives from a diverse set of organizations that operate the North American energy sector [1]. The electricity subsector version of the C2M2 (ES-C2M2) has been widely and successfully used by energy organizations and facilities in the North American energy sector for over five years, including for a wide range of energy generating assets. Slightly modified versions of the ES-C2M2 are used for different types of energy facilities—different versions of the C2M2 exist to evaluate the cybersecurity programs at hydroelectric dams and oil and natural gas facilities. Nuclear facilities can be assessed using the energy sector or generic version of the C2M2; however, a specialized version that focuses on nuclear facilities could be easily developed by modifying the ES-C2M2.

2. MATURITY MODEL BACKGROUND

As described in [1], a “maturity model” is a set of indicators, characteristics, or attributes that designate capability and progression in the given subject area being assessed. The model incorporates laws, standards, guidance documents, industry good (and best) practices, lessons learned, and other measures of maturity. A maturity model provides a way to benchmark a government, industry, or facility organization’s nuclear cybersecurity program by evaluating the current or planned level of capability of its practices, processes, and methods. The model can be used within an organization to set short- or long-term goals and establish priorities for making programmatic enhancements. For government agencies, a maturity model can identify areas where additional regulations, guidance, inspections, or assistance activities might be beneficial and cost effective. For industry associations it can identify areas that might warrant more technical guidance, information sharing among industry members, and technical training. If industry members approve, industry associations can provide a forum for nuclear facilities to share maturity model results to allow its members to benchmark their performance and identify superior practices that can be adopted by the broader nuclear community. For nuclear facilities or the organizations that manage those facilities, a maturity model can be used to identify programmatic areas in their organizations or facilities that warrant more (or less) attention based on risk.

3. C2M2 MATURITY INDICATOR LEVELS

The C2M2 and ES-C2M2 evaluate maturity in ten security domains. For nuclear organizations, these domains can be summarized as follows:

- Risk Management (RM) – identify, analyse, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.
- Asset, Change, and Configuration Management (ACM) – manage digital assets (including operational and information technology assets and their associated hardware and software) commensurate with risk to the organizational cybersecurity goals.
- Identity and Access Management (IAM) – create and manage identities for entities and individuals that may need logical or physical access to the organization’s assets. Control access to the organization’s assets commensurate with the risk to critical infrastructure and organizational objectives.
- Threat and Vulnerability Management (TVM) – establish and maintain plans, procedures, and technologies to detect, identify, analyse, manage, and respond to cybersecurity threats and vulnerabilities commensurate with the risk to the organization and the organization’s cybersecurity objectives.
- Situational Awareness (SA) – establish and maintain activities and technologies to collect, analyse, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture.

- Information Sharing and Communications (ISC) – establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including up-to-date information on threats and vulnerabilities, in order to characterize and reduce risks and increase operational resilience commensurate with the risk to nuclear facilities and materials and organizational security objectives.
- Event and Incident Response, Continuity of Operations (IR) – establish and maintain plans, procedures, and technologies to detect, analyse, and respond to cybersecurity events and sustain operations throughout a cybersecurity event, commensurate with the risk to nuclear facilities and materials and organizational objectives.
- Supply Chain and External Dependencies Management (SCM) – establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities commensurate with the risk to nuclear facilities and materials and organizational objectives.
- Workforce Management (WM) – establish and maintain plans, procedures, technologies, and controls to create a cybersecurity culture and ensure the ongoing suitability and competence of personnel commensurate with the risk to nuclear facilities and materials and organizational objectives.
- Cybersecurity Program Management (CPM) – establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and security risks [1].

In each domain, individual programmatic security practices are provided and organized into one or more cybersecurity objectives. The practices are the key programmatic activities used to evaluate performance at different levels of programmatic maturity. To measure the progression of cybersecurity performance, maturity models typically have a scale of maturity levels. The C2M2 family of models use four levels of maturity [1]. The maturity levels and their characteristics are:

Maturity Indicator Level 0 (MIL0) is the lowest level of maturity. The model specifies no practices for MIL0. An organization achieves a MIL0 level as a default starting point even if it does not conduct any activities characterized by the practices [1].

Maturity Indicator Level 1 (MIL1) is the next higher level of maturity. To achieve MIL1 in each domain, a set of initial practices must be achieved. At MIL1, many practices only have to be performed in an informal or ad hoc manner. MIL1 is generally achieved because of the cybersecurity interest or experience of an individual or team, without much in the way of organizational guidance in the form of a prescribed plan or policy covering the associated cybersecurity activity or to provide associated cybersecurity training. The quality of ad hoc activities may vary significantly depending on who performs the activities, when they are performed, how they are performed, and the priority and resources assigned to the activities. With experienced and talented personnel, high-quality outcomes may be achieved even if practices are performed in an ad hoc manner. However, at this level, lessons learned are typically not captured by the organization so approaches and outcomes may change suddenly as personnel and management priorities change for undocumented activities [1].

Maturity Indicator Level 2 (MIL2) has four management levels of performance: (1) practices are performed according to a documented plan and the work done to implement the practices are documented; (2) stakeholders for the practices are identified and involved in the performance of the practices, which may involve stakeholders from different portions of the organization or facility or from outside the organization or facility; (3) adequate resources are provided to support the practices, including people, tools, and funding (to allow staff to devote time to performing the practices); and (4) standards and/or guidelines have been identified to implement the practices and may be international, national, industry, or organizational. Overall, the practices at MIL2 are more complete than at MIL1. At MIL2, the organization can be more confident that the performance of the domain practices will be sustained over time [1].

At Maturity Indicator Level 3 (MIL3) cybersecurity programmatic activities are more thoroughly managed and their implementation has been institutionalized within the relative portions of the organization. Five general categories of activities support this this maturity level: (1) activities are guided by policies and other types of organizational or governance directives and the policies are an extension of the planning activities that are in place at MIL2; (2) policies include compliance requirements for addressing applicable standards or guidance; (3) activities are reviewed at a frequency defined by the organization to ensure applicable policies are being properly implemented by staff and contractors; (4) roles, responsibilities, and authorities for performing cybersecurity practices are assigned and understood; and (5) personnel performing the practices have the skills and knowledge to perform their assignments. At MIL3, the organization should demonstrate the ability to sustain a high level of performance in each of the specified practices regardless of changes in personnel [1].

These levels apply independently to each domain. As a result, an organization using the model may be operating at different MIL ratings for different domains. For example, an organization could be operating at MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain. Establishing a target MIL for each domain is an effective strategy for using the model to guide cybersecurity program improvement. Organizations should become familiar with the practices in the model prior to determining target MILs. Improvement efforts should then focus on achieving those target levels. Performance and MIL achievement need to align with business objectives and the organization's cybersecurity strategy. Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL against potential benefits. However, the model was developed so that all companies, regardless of size, could achieve MIL1 across all domains.

To determine cybersecurity maturity levels each practice in the C2M2 family of models is evaluated using four scoring options:

(a) Fully implemented. The practice is complete, and all activities associated with all aspects of the practice are implemented or are ongoing.
(b) Largely implemented. The practice is well on the way to being complete. Most activities associated with the practice and all aspects of the practice are implemented, ongoing, or scheduled for timely implementation. No key activities associated with the practice are ignored.
(c) Partially implemented. Some activities associated with the practice are implemented, ongoing, or scheduled for timely implementation, but other activities needed to achieve this practice are ongoing or planned.
(d) Not Implemented. No progress has been made in implementing the practice [1].

When determining the overall maturity level of a nuclear facility's cybersecurity program within a domain, all the MIL1 practices must be achieved at the fully or largely implemented level to achieve an overall MIL1 designation for that domain. If even one practice at the MIL1 is partly or not implemented, MIL1 is not achieved and the overall maturity level for the domain is designated MIL0. All the MIL1 and MIL2 practices must be achieved at the fully or largely implemented level in a domain to achieve an overall MIL2 designation for that domain. Similarly, all the MIL1, MIL2, and MIL3 practices must be achieved at the fully or largely implemented level in a domain to achieve an overall MIL3 designation for that domain.

4. C2M2 RESULT REPORTING

The C2M2 can be completed and an Evaluation Report produced using an Excel workbook distributed by the DOE. An online C2M2 tool is also available from Pacific Northwest National Laboratory. The Evaluation Report provides automated text output, including background information on the C2M2 and its domains and practices. It also provides graphical representations to support data analytics. The facilitator will use the C2M2 Evaluation Scoring Report to support an end-of-assessment briefing to facility management and staff. A key graphical output product in any post-assessment report is a summary presentation of maturity assessment results. Fig. 1 presents an example of this summary product [2]. It presents a 3x10 array of “donut charts” with a separate donut for each domain and maturity level.

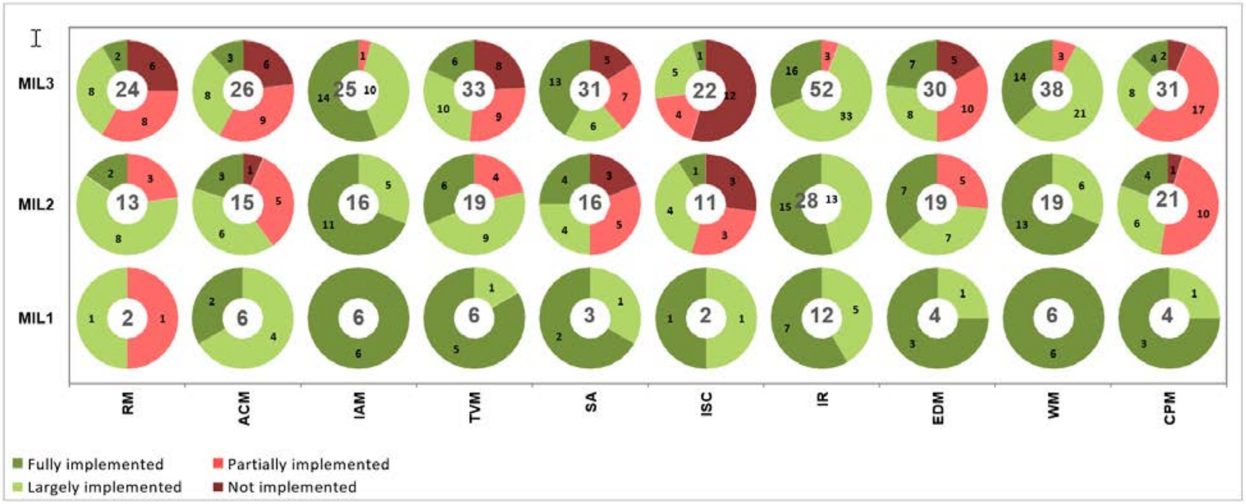

FIG. 1. Graphical summary of the C2M2 results

In each of the 30 coloured donuts displayed in Fig. 1, red sectors provide a count of the number of applicable practices that received responses of “Not Implemented” (dark red) or “Partially Implemented” (light red). Red shading indicates practices that prevented the organization for achieving the associated MIL. Green-shaded sectors show the number of questions that received responses of “Largely Implemented” (light green) or “Fully Implemented” (dark green). Donuts that are all green indicate the corresponding MIL is achieved for that domain. The number in the centre of the donut indicates the cumulative number of practices that must be answered “Largely Implemented” or “Fully Implemented” to achieve that MIL. Because the process of achieving a maturity level is cumulative, the number in the centre of the donuts for MIL3 includes the number of total practices for that domain, including all the MIL1, MIL2, and MIL3 practices. Similarly, the number in the centre of the donut for MIL2 includes the number of MIL1 and MIL2 practices for that domain [2].

A quick inspection of the example in Fig. 1 indicates that one domain (Risk Management) does not achieve MIL1; it defaults to MIL0 because one of its two MIL1 practices is still only Partly Implemented. Six domains achieve MIL1 (ACM, TVM, SA, ISC, EDM, CPM) but do not achieve MIL2. Three domains achieve MIL 2 (IAM, IR, and WM), but do not achieve MIL3. Each of domains achieving MIL2 have between one and three practices at MIL3 that are only partly implemented. It might take only a few changes to adequately address these red-shaded practices to elevate the cybersecurity programmatic performance to the top maturity level. The organization may elect to do so, or from a risk management perspective, its resources might best be spent to raise the RM domains maturity to MIL1 and MIL2 and raise other domains that only scored MIL1 to MIL2 [2].

Achieving the highest possible MIL scores is not the goal of most organizations performing a C2M2 analysis. Investments in cybersecurity beyond what is required to meet regulatory requirements is a risk management decision. The organization needs to address the question, “What additional investment in cybersecurity programmatic areas makes sense from a benefit to cost perspective?” That decision should consider the likelihood of a successful cyberattack as well as the consequences involving safety, security of the facility and materials, continuity of business, protection of intellectual property, government action, and public perception that could result from a successful cyberattack. Regardless of the risk management decisions eventually made, simply having the characterization of programmatic cybersecurity maturity by domain can be extremely useful for an organization to support situational analysis, information sharing, and future decision making.

5. SCREENING VERSION OF THE C2M2 FOR NUCLEAR CYBERSECURITY

The cybersecurity maturity screening model (CMSM) is designed to provide a rapid preliminary assessment of the relative maturity of a foreign country's government, industry supported, and site implemented nuclear cybersecurity program, including identifying areas of strengths and weaknesses. The CMSM is a slimmed down version of the C2M2. Three versions of this screening model are available, one each for evaluating:

- Government cybersecurity regulations, regulatory actions, and technical support to the nuclear sector;
- Industry support to the government and nuclear facilities (as provided by nuclear industry, energy sector, or academic associations);
- Cybersecurity programmatic implementation by organizations at nuclear facilities.

Each model examines cybersecurity practices in five domains of interest. The domains are based on the Nuclear Threat Initiative cybersecurity Nuclear Security Index (https:/ntiindex.org/indicators/security-and-control-measures/) and are roughly as follows for the purposes of the CMSM:

(a) Mandatory Cybersecurity – Evaluate domestic laws, regulations, or licensing rules requiring nuclear facilities to have protection from a cyberattack. Evaluate how well government, industry, or nuclear facilities achieve implementation.

(b) Critical Asset Protection – Evaluate domestic laws, regulations, or licensing rules requiring nuclear facilities to identify critical digital assets and protect them from a cyberattack. Evaluate how well government, industry, or nuclear facilities achieve implementation. Critical digital assets include the following systems and networks:

   (1) Safety-related functions
   (2) Security functions
   (3) Emergency preparedness functions
   (4) Support systems and equipment related to the above functions.

(c) Threat and Vulnerability – Evaluate requirements and support for cyber threat assessments or design basis threat for nuclear facilities. Evaluate how government, industry, and sites achieve their threat assessment goals.

(d) Inspections and Assessments – Evaluate the performance-based cybersecurity inspection or assessment program, including assessments of cybersecurity program implementation at nuclear facilities. Evaluate how well government, industry, or sites prepare for and conducted inspections and self-assessments.

(e) Incident Response – Evaluate domestic laws, regulations, or licensing requirements associated with cybersecurity incident response plans for nuclear facilities. Evaluate how well government, industry, and sites support incident response goals.

With a reduced number of domains and practices (about 1/7 the number of practices) the screening model should take well under an hour for an informed evaluator to complete an assessment.

6. CONCLUSIONS AND PROPOSED COURSE OF ACTION

Maturity models can provide government agencies, industry associations, and organizations operating nuclear facilities with the ability to quickly evaluate the maturity of their cybersecurity programs and identify programmatic areas they may wish to prioritize for improvement. The C2M2 family of maturity models have a proven track record of supporting organizations in the North American energy sector and other critical infrastructure in evaluating the programmatic maturity of their cybersecurity program. The model is designed to be readily applied and an assessment can be completed in one to several days (depending on the availability of information) by one individual. New maturity models built on the C2M2 framework are addressing the cybersecurity of building systems, supply chain security, transmission system resilience, and other applications. The current version of the ES-C2M2 can be used to assess nuclear facilities and it is proposed to develop a customized version of the C2M2 for nuclear facility applications that can provide even more relevant information.

A screening version, the CMSM, is designed to provide a rapid preliminary assessment of the relative maturity of a foreign country's government, industry supported, and site implemented nuclear cybersecurity program, including identifying areas of strengths and weaknesses. An assessment with this screening model can be completed in less than an hour. The CMSM is in the testing stage and there are plans to release it for international use.

REFERENCES

[1] U.S DEPARTMENT OF ENERGY, Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1, Washington, D.C. (2014a), http:/energy.gov/node/369271

[2] U.S DEPARTMENT OF ENERGY, Electricity Subsector Cybersecurity Capability Maturity Model Facilitator Guide (ES-C2M2), Version 1.1, Washington, D.C. (2014b), https:/www.energy.gov/sites/prod/files/2017/04/f34/2017-03-21-C2M2%20Facilitator%20Guide%20v1.1a.pdf