Contribution ID: **537** Type: **Paper**

The Application of Maturity Models for Evaluating Computer Security Programs at Nuclear and Radiological Facilities

Maturity models, like the Cybersecurity Capability Maturity Model (C2M2), are applicable for nuclear and radiological facilities. The C2M2 was developed by the U.S. Department of Energy to allow critical infrastructure organizations to evaluate the general capabilities of their computer security programs in a consistent manner, communicate capability levels in meaningful terms, prioritize computer security investments for targeted areas of concern, and track how the maturity of their computer security program is changing over time. The C2M2 is designed for use by any critical infrastructure organization—regardless of ownership, structure, or size. Broad use of the C2M2 and the sharing of C2M2 results enables organizations in the United States to benchmark their performance. The C2M2 and similar maturity models are designed to be quick and easy to use. It can take as little as an hour or as much as a few days to complete a C2M2 analysis –with the amount of time dependent on the size and complexity of an organization/facility and its computer security program. The C2M2, or similar computer security maturity models, can help decision makers at nuclear and radiological facilities understand the status of their computer security program, set goals for the future, and make risk-informed decisions on how to achieve their computer security goals.

The C2M2 or similar maturity models may be used at multiple levels within a nuclear or radiological facility. For example, C2M2 results may be used operationally by:
• Decision makers who control the allocation of resources and are responsible for the management of security risks for the entire organization (not just its nuclear and radiological facilities)
• Managers responsible for a nuclear or radiological facility's operations, safety, and security
• Security, computer security, and information technology professionals at a nuclear or radiological facility
• Staff members responsible for conducting computer security self-evaluations at a facility.

The C2M2 is built on a foundation of existing computer security standards, frameworks, programs, and initiatives. The model features 10 security domains; examples of which include Identity and Access Management, Threat and Vulnerability Management, Supply Chain and External Dependencies Management, and Workforce Management. Performance in each security domain is characterized using a structured set of practices. The practices represent activities an organization can perform to improve computer security in their domain. For example, the Workforce Management domain is composed of practices that an organization can perform to establish and enhance its workforce's computer security capabilities. Sample practices include:
• Computer security responsibilities are assigned to specific people.
• Security vetting is performed at an organization-defined frequency for personnel with access to key digital assets.
• Computer security training is provided as a prerequisite to granting access to digital assets.
• Computer security awareness activities are conducted to reinforce training.

The C2M2 defines four maturity indicator levels, 0 through 3, which apply independently to each domain in the model. To earn a maturity level in a given domain, an organization must perform all of the practices for that maturity level and its predecessor level(s). For example, an organization must fully or largely achieve all the practices prescribed for maturity level 1 and 2 to achieve an overall maturity level of 2 in that security domain.

Striving to achieve the highest maturity level in all domains may not be the optimal business solution. For example, a small facility that manufactures radiopharmaceuticals may be able to overcome the consequences of a successful cyberattack better than a nuclear facility (as the competent authority may shut down the nuclear facility for weeks or months longer than the radiopharmaceutical facility owing to the greater safety and security risk (and stakeholder interest) associated with an incident at a nuclear facility. In such a case, the computer security maturity level that is the goal of the organization operating the radiopharmaceutical facility may be somewhat less than the goal for the nuclear facility.

A given organization or facility might value performance in some security domains more than others. The C2M2 provides flexibility for an organization to target different maturity levels for its security domains based upon its defined business objectives. The benefits and costs of computer security programmatic activities should be evaluated against the risks and costs of a successful cyberattack when selecting appropriate goals for a nuclear or radiological facility's computer security maturity levels. This paper will report on the application of computer security maturity models for nuclear and radiological facilities and illustrate how these models

can be used to guide planning for computer security programs.

State

United States

Gender

Primary author: GLANTZ, Clifford (Pacific Northwest National Laboratory)

Co-authors: SKARE, Paul (Pacific Northwest National Laboratory); LANDINE, Guy (Pacific Northwest National Laboratory); GOURISETTI, Sri Nikhil Gupta (Pacific Northwest National Laboratory); MYLREA, Michael (Pacific Northwest National Laboratory)

Presenter: GLANTZ, Clifford (Pacific Northwest National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security