Evaluating the Maturity of Cybersecurity Programs for Building Control Systems

Clifford Glantz, Sriram Somasundaram, Michael Mylrea, Ron Underhill, and Andrew Nicholls, Pacific Northwest National Laboratory

ABSTRACT

The cyber-physical security threat to buildings is complex, non-linear, and rapidly evolving as operational and information technologies converge and connect buildings to cyberspace (Mylrea, 2015). Cyberattacks on buildings can exploit building controls and breach corporate networks, causing physical, financial and reputational damage. This may result in the loss, disruption, manipulation and damage to sensitive financial and building information, including systems necessary for the safe and efficient operation of buildings. A robust national cybersecurity strategy for buildings, including actionable guidance on the selection and implementation of appropriate cybersecurity controls for buildings, and an approach to evaluate the maturity and adequacy of cybersecurity programs are needed to protect critical infrastructure.

To provide an approach for evaluating the maturity of the cybersecurity programs for building control systems, the US Department of Energy's widely used Cybersecurity Capability and Maturity Model (C2M2) has been adapted into a version examining critical cyber assets and controls in buildings. The revised model, the Buildings-C2M2 (B-C2M2) provides maturity level indicators for cybersecurity programmatic domains. A "B-C2M2 Lite" version allows facility managers and building control system engineers, or information technology personnel to perform rapid self-assessments of their cybersecurity program. Both tools have been pilot-tested on several facilities. This paper outlines the concept of a maturity model, describes the B-C2M2 tools, presents results and observations from the pilot assessments, and lays out plans for future work.

Introduction

Cyberattacks are a growing threat to critical infrastructure around the world. Proactive and coordinated efforts are necessary to strengthen and maintain resilient critical infrastructure that reside in facilities and buildings (Interagency Security Committee 2015). As buildings and facilities involved in energy, health care, transportation, finance, chemical, communications, defense, government, manufacturing, and other commercial sectors increasing rely on automated control systems, they are increasingly vulnerable to cyberattacks. Managers, control system engineers, and information technology (IT) personnel who support building operations (e.g., electrical power, heating/cooling/ventilation, lighting, potable water, wastewater, fire detection and suppression, transportation, security monitoring, and security and safety alarms) need to consider cybersecurity issues to ensure that the advances in efficiency and productivity associated with automated control systems are not jeopardized by cyber vulnerabilities. One of the first steps in addressing this concern is to evaluate the maturity of the cybersecurity programmatic framework that is governing building control systems. This evaluation allows decision makers to identify areas of potential strength and weakness in the security program covering their building control systems and evaluate if, or what security domains warrant additional attention.

In this paper, the authors report on the development of a Building Cybersecurity Capability Maturity Model (B-C2M2) that allows building managers and their staff to perform a rapid (1–2 hours) and inexpensive initial assessment of their cybersecurity program. The B-C2M2 was developed by Pacific Northwest National Laboratory (PNNL) under the sponsorship of the Federal Energy Management Program and Building Technologies Office in the US Department of Energy (DOE) Office of Electrical Efficiency and Renewable Energy (EERE). It is based on the successful application of the C2M2 concept developed for energy sector utilities to evaluate their overall cybersecurity program (DOE 2014). The B-C2M2 can be used to benchmark the status of diverse building stakeholders' cybersecurity program, identify programmatic strengths and weaknesses, raise awareness of cybersecurity risks, and promote the application of enterprise-level cybersecurity controls to building control systems. The application of the B-C2M2 during a series of field pilot assessments provides interesting insights on the state of building control system cybersecurity. The pilot assessments also assisted in enhancing the assessment criteria and ease-of-use of the B-C2M2.

The Cyber Threat to Building Control Systems

The scope of cyberattacks is evolving as industrial control systems are increasingly digitized and networked and attackers are expanding into the cyber-physical realm. In testimony before the US House Committee on Intelligence on September 10, 2015, James Clapper, Director of National Intelligence, said "Politically motivated cyberattacks are now a growing reality, and foreign actors are reconnoitering and developing access to US critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile. In addition, those conducting cyber espionage are targeting US government, military, and commercial networks on a daily basis." (Clapper 2015). Hacktivists, criminals, and disgruntled insiders also pose a substantial cyber threat.

Cyberattacks can compromise the confidentiality of information, the availability of information and operational technology assets, and the integrity of those assets that support the efficient and reliable operation of buildings and facilities. The capabilities of attackers are growing more sophisticated. Attack tools are developed by a range of malicious actors, from highly skilled individuals to well-financed nation states and criminal organizations. Attack tools and training are available for free online. Sophisticated cyberattack tools are also sold on the cyber black market, enabling less-skilled individuals to acquire substantial cyberattack capabilities. The cyber black market, "once a varied landscape of discrete, *ad hoc* networks of individuals motivated by ego and notoriety, has now become a burgeoning powerhouse of highly organized groups, often connected with traditional crime groups (e.g., drug cartels, mafias, terrorist cells) and nation-states." (Albion et al. 2014).

Many buildings are using automated control systems, and linking them to IT enterprise networks to enable system-wide decision making, execution, and optimization. The equipment and devices that are linked together span a range of complexity and cost. Yet a weakness in one linked element in the building (e.g., an inadequately protected access point, vulnerabilities in software or operating systems, or inadequate or inappropriate security-related decisions by building staff) can jeopardize the security and reliability of building systems.

For buildings and facility infrastructure, a robust building cybersecurity strategy is needed to plan, protect, and safeguard communication systems, control systems, and physical properties—and the building owners and occupants who rely upon them every day. A dialog on the appropriate set of cybersecurity controls for buildings and facilities is also needed. This dialog would provide support for the development of a balanced and risk-based set of management, operational, and technical cybersecurity controls for an integrated cybersecurity program. Decision makers need to understand what their cybersecurity program can achieve in reducing risks to building operations. They also need to understand the cost to procure, install, operate, and maintain their cybersecurity program—as well as the potential loss-of-productivity costs that may be associated with implementing a comprehensive program.

Initiatives to Address the Cyber Threat to Building Control Systems

To address cyber threats, DOE EERE supports a number of projects to enhance the cybersecurity of building control systems as it supports continued efforts to enhance energy efficiency. Three major thrust areas are:

- Develop a robust national cybersecurity strategy for buildings. This includes developing a streamlined cybersecurity framework for buildings that is compatible with the National Framework for Improving Critical Infrastructure Security (78 FR 11739-11744).
- Provide guidance on the selection and implementation of appropriate cybersecurity controls for buildings. This includes information on the potential risk reduction and cost of security control options.
- Provide tools to evaluate the maturity of the cybersecurity programs protecting building systems.

The development and application of the B-C2M2 is directly related to the third bullet. The B-C2M2 provides an efficient and effective way to foster cybersecurity situational awareness. It encourages the development of cybersecurity risk management plans, policies and procedures for building systems. It is also designed to support and be integrated with other activities that are currently under way to protect building systems.

The Cybersecurity Capability Maturity Model and its Application to Building and Facility Systems

A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. The model provides a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods. Results can be used to set goals and priorities for improvement (DOE 2014). When a maturity model is widely used by similar types of buildings or facilities—and model results are shared (often in a manner that protects the anonymity of a given building or facility—organizations can benchmark their performance against their peers.

The Cybersecurity Maturity Model

To classify the maturity of cybersecurity programs, models typically use discrete "maturity levels." A set of attributes is specified for each maturity level. If an organization demonstrates the attributes for that level, it has achieved or surpassed that maturity level. Having attributes for each level enables an organization to evaluate its performance against those attributes to define its current maturity level and identify what it needs to do to attain a higher level of maturity (DOE 2014)

The C2M2 was originally developed in support of the Electricity Subsector Cybersecurity Risk Management Maturity Initiative, a White House initiative led by the DOE in partnership with the US Department of Homeland Security (DHS). This development activity was conducted in collaboration with private- and public-sector experts, representatives of asset owners within the electricity subsector, and the operators of electricity subsector assets (including generation, transmission, and distribution assets) (DOE 2014). The initiative used the National Infrastructure Protection Plan framework as a public–private partnership mechanism to support the development of the model. The initiative leveraged and built upon existing efforts, models, and cybersecurity best practices and is aligned with the *Cyberspace Policy Review* (White House 2010), *Roadmap to Achieve Energy Delivery Systems Cybersecurity* (DOE 2011), and *Cross-Sector Roadmap for Cybersecurity of Control Systems* (DHS 2011). DOE has been successful in gaining wide usage of the C2M2 within the electricity subsector and the oil and gas subsector.

The C2M2 assessment process does not include an actual inspection of equipment because it is focused on the cybersecurity program, not the detailed technical aspects of cybersecurity. The C2M2 is purely an interview-based question-and-answer process. The C2M2's questions are organized into 10 security domains, with each security domain focusing on a logical grouping of cybersecurity practices. The domains, as described by DOE (2014), are:

- Risk Management (RM). Establish, operate, and maintain a cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk.
- Asset, Change, and Configuration Management (ACM). Manage the organization's IT and control system assets, including both hardware and software.
- Identity and Access Management (IAM). Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets.
- Threat and Vulnerability Management (TVM). Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities.
- Situational Awareness (SA). Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information 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 threats and vulnerabilities.
- Event and Incident Response/Continuity of Operations (IR). Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event.
- Supply Chain and External Dependencies Management (EDM). Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities.
- Workforce Management (WM). Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel.
- Cybersecurity Program Management (CPM). Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities.

The C2M2 defines four maturity indicator levels (MILs), ranging from 0 to 3 (DOE 2014). The maturity indicator levels apply independently to each security domain. As a result, an organization using the C2M2 may be operating at different MIL ratings for different domains.

MIL1 contains a set of initial practices for each security domain. To achieve MIL1, the initial activities may be performed in an informal or *ad hoc* manner, but they must be performed. If an organization were to start with no capability in managing cybersecurity, it should focus initially on implementing the MIL1 practices. MIL2 has its own set of practices that build upon MIL1. At MIL2, cybersecurity practices are documented, stakeholders are identified and involved, adequate resources are allocated to support processes, and guidelines have been identified to guide implementation. At MIL3, activities are guided by policies (including compliance requirements), activities are periodically reviewed to ensure they conform to policy, responsibility and authority for performing practices are assigned to personnel, and personnel performing the practices have adequate skills and knowledge (DOE 2014).

The MILs are cumulative within each domain; to earn a MIL1, 2, or 3 in a given domain, an organization must perform all of the practices in that level and its predecessor level(s) (DOE 2014). Performance of practices is evaluated using a series of questions. A total of 312 questions make up the C2M2. Questions focus on evaluating specific aspects of a practice. Questions are designed to be answered one of four ways: not implemented, partially implemented, largely implemented, and fully implemented. Answers of “largely implemented” or “fully implemented” receive credit for achieving a practice. An answer of “not implemented” or “partially implemented” will prevent a MIL level from being achieved (DOE 2014).

The Building Systems Cybersecurity Maturity Model

The B-C2M2 is based on the C2M2. B-C2M2 uses the same security domains and practices for evaluating the maturity of cybersecurity programs for building control systems but the questions are altered to fit the needs of the building control system community. Further, the B-C2M2 is offered in a “Lite” version that shortens the assessment process and requires fewer questions. A major element of shortening of the assessment process was achieved by cascading the questions. If a “not implemented” answer was received for some key questions, quite a few questions could be skipped, because those questions would also have to produce a “not implemented” response. Use of the Lite version of the B-C2M2 reduced the time and complexity of an assessment, setting the stage for its future use as a non-facilitated assessment tool. For most buildings and many multiple-building facilities, the B-C2M2 Lite assessment could be completed in less than an hour. For complex buildings, or facilities with a greater number and array of buildings, the assessment was generally completed in less than two hours.

It is up to the building or facility using the B-C2M2, to decide which staff members to involve in the assessment. The facility/building manager, a building control system engineer, and an IT person are useful in providing informed input for the assessment. At some facilities, multiple building control system engineers may be involved because they maintain different sets of building control systems that may have different levels of cybersecurity. In addition, there may be other personnel who should be involved because they might have cybersecurity responsibilities directly related to a building’s control systems.

Results from a B-C2M2 assessment can be used in a timely manner by senior management, those participating in the assessment, and their colleagues. Senior decision makers, who may be enterprise-level managers (e.g., senior corporate officers, program managers), may use assessment information to:

- Determine if the current cybersecurity program for building control systems has sufficient maturity, given the identified cybersecurity risk.
- Set future maturity level targets for cybersecurity for its building control systems.

- Allocate additional resources (e.g., budget, people, and equipment) to address identified gaps or weaknesses in cybersecurity program.
- Require the development and implementation of enterprise-level policies and procedures governing building control system security.

Facility managers may, within their own building(s), use assessment information to:

- Adjust cybersecurity priorities to achieve maturity goals.
- Direct staff to conduct cybersecurity activities that address programmatic shortfalls.
- Adjust resource allocations (e.g., budget or staff) to address cybersecurity issues.
- Develop written policies and procedures governing building control system security.
- Adjust staff activities, goals, and evaluation criteria to incorporate activities associated with cybersecurity activities.

Building control system engineers may use assessment information to:

- Increase the attention they pay to monitoring cybersecurity threats, attack pathways, vulnerabilities, and security solutions.
- Allocate more time to reviewing and monitoring potential cybersecurity issues.
- Increase configuration management activities and timely security patching.
- Restrict access to building control systems.
- Closely monitor the cybersecurity programs of their vendors, suppliers, and contractors. This includes access to building control systems and operations performed on the systems.
- Identify and evaluate the personnel security status of staff members and suppliers who are maintaining or reconfiguring building control systems.

IT personnel may use assessment information to:

- Increase their awareness of potential cybersecurity issues and vulnerabilities involving building control systems.
- Incorporate building control system security into their enterprise cybersecurity activities.
- Conduct cybersecurity scanning and assessment activities on building control systems.
- Investigate, and upgrade as needed, the defensive architecture protecting building control systems.
- Investigate network segmentation between the enterprise network and building control systems to ensure that unnecessary connections do not exist.

Pilot Assessments and Observations

From October 2015 through February 2016, the B-C2M2 was used to conduct assessments at four different pilot facilities:

- A large radiochemical processing research facility. The facility contained many automated building control systems. Radiological safety and security are a priority at this facility.
- A local government’s city hall building. It houses government offices and services in support of a community with about 50,000 residents. The building, of recent construction, features state-of-the-art energy and other building control systems.
- A small, state urban university system campus with a mix of buildings (constructed between the 1970s and 2015), many with automated building control systems.
- A community college campus with a mix of buildings (constructed between the late 1950s

and 2010s). The college has partnered with a major control system supplier to implement a college-wide energy efficiency project.

The identities of the pilot facilities and their detailed assessment data are kept confidential. Only the authors have that data and it is not shared with the project sponsors.

To conduct the assessment at each facility, the B-C2M2 team representative met with the building staff to perform the assessment interview. Typically, the building facility manager participated, along with one or more building control system engineers, and one IT enterprise program representative.

Figure 1 presents the summary B-C2M2 results for the pilot site with the highest cybersecurity programmatic maturity of the four pilot sites. Results for each of the 10 security domains and the three MIL levels are presented in 30 colored pie charts. The number within the center of each pie chart indicates the number of questions that need to be answered affirmatively to reach that MIL level. Color coding within the pie charts indicates the frequency of the answers registered for the evaluation questions. Dark green represents an answer of "fully implemented" and light green is "largely implemented;" these are affirmative answers for achieving a MIL level. Light red is "partially implemented" and dark red is "not implemented;" these are answers that prevent a MIL level from being achieved.

The MIL1 pie chart for Risk Management (RM), as found in the lower left corner of the Figure 2, indicates two evaluation questions are used to assess MIL1 status. The dark green color of the pie chart indicates that the two evaluation items are assessed as "fully implemented." Therefore, MIL1 level has been achieved for RM. The MIL2 pie chart for the RM domain has 13 evaluation questions that need to be addressed—this includes the two questions assessed for MIL1 and 11 others that apply to MIL2. This pie chart shows that MIL2 is not achieved because four of the 11 evaluation questions are answered as only "partly implemented."

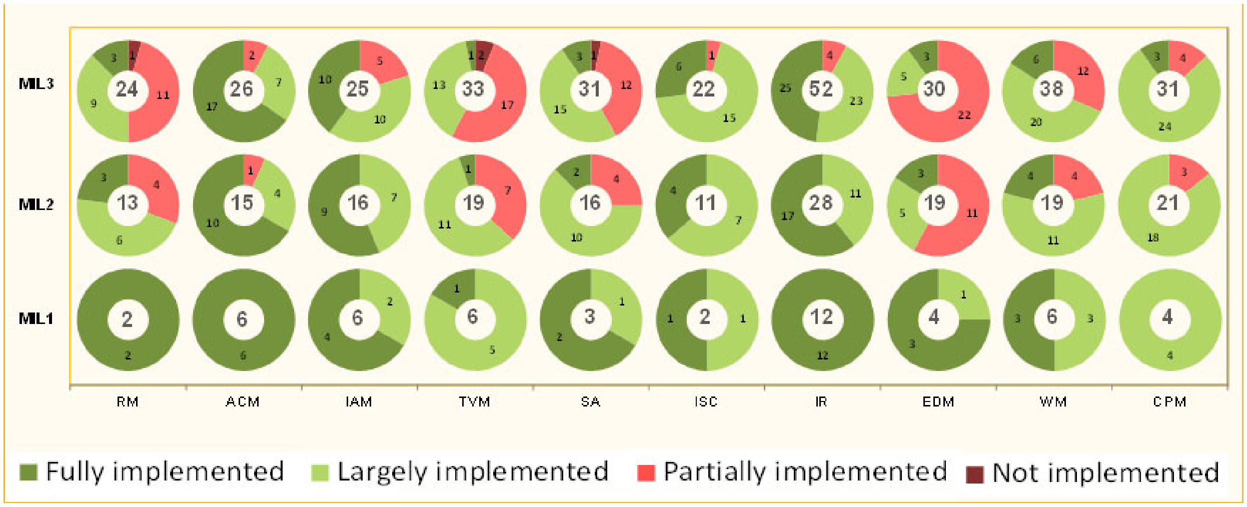

Figure 1. Summary of the maturity level evaluation for the pilot assessment site with the highest cybersecurity programmatic maturity for its building control systems.

In summary, Figure 1 shows that this pilot site achieves at least MIL1 in all of the domains, MIL2 in three domains, and no security domain achieves MIL3. Several security domains have only a few "partly implemented" responses. If these few items are more thoroughly addressed by facility management and staff, MIL2 could be readily achieved. One security domain, Information Sharing and Communications (ISC) has only one evaluation item preventing it from achieving a MIL3 score. For two other domains, a MIL3 score would require the staff to successfully address only a few unmet evaluation items.

Figure 2 presents an alternative summary display for this site. Less information is provided, but the maturity levels achieved for each security domain are more readily compared.

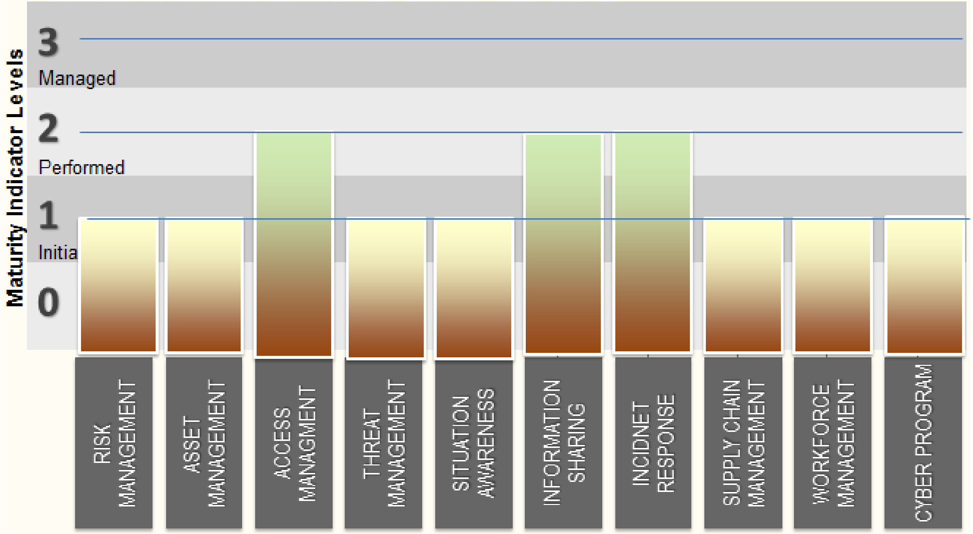

Figure 2. Simple summary presentation of the maturity level results of the pilot assessment site with the highest cybersecurity programmatic maturity for its building control systems.

Figure 3 presents the summary B-C2M2 results for the pilot site with the lowest cybersecurity programmatic maturity of the four pilot sites. Only three of the security domains achieve MIL1. The other six security domains achieve only MIL0. One of these domains has only one "partly implemented" response that is keeping it from achieving MIL1. This result indicates that in many security domains, undocumented or *ad hoc* activities are not conducted to support key cybersecurity activities for the protection the building control systems.

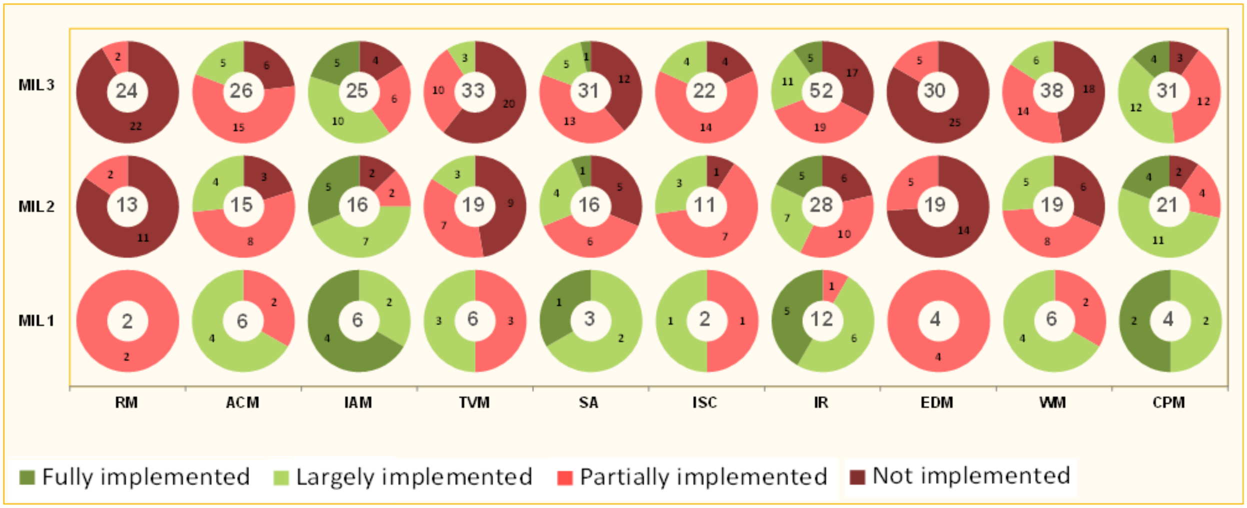

Figure 3. Summary of the maturity level evaluation for the pilot assessment site with the lowest cybersecurity programmatic maturity for its building control systems.

Figure 4 presents an alternative summary display for this site. Less information is provided, but the maturity levels achieved for each security domain are more readily compared.

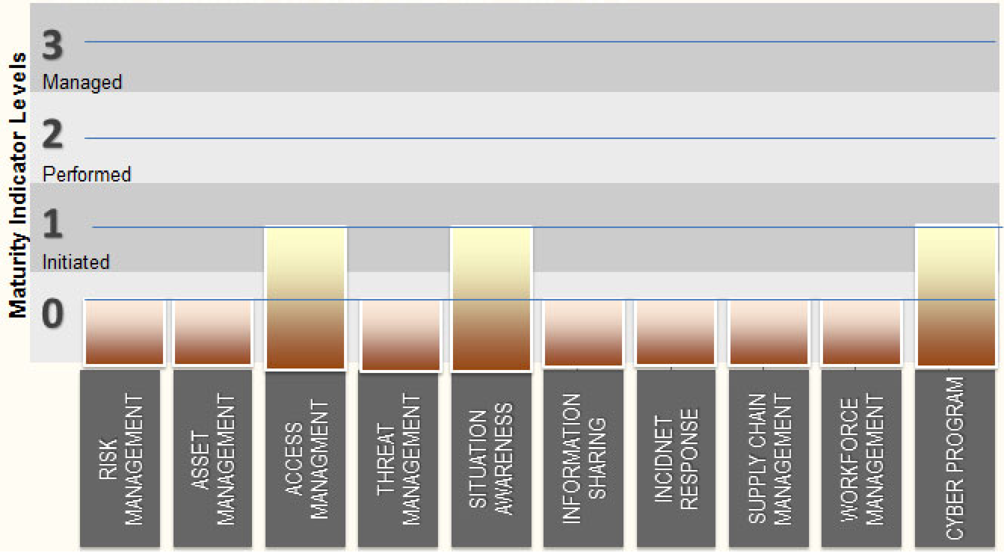

Figure 4. Simple summary presentation of the maturity level results the of pilot assessment site with the lowest cybersecurity programmatic maturity for its building control systems.

The difference in the maturity of the cybersecurity programs for the building control systems at the four pilot sites was not surprising. Cybersecurity maturity goals need to be risk-based. Facilities that could experience substantial consequences from a cyber compromise of their building control systems (e.g., loss of life from explosion or fire, loss of security resulting in theft or sabotage, or large business costs from loss of building use or degradation in its operations) should require a high maturity level in all of its security domains. Facilities that would experience only negligible consequences (e.g., limited loss of building operations with no major impact on occupants) could readily tolerate low maturity levels. After determining their current cybersecurity programmatic maturity for their building control systems, facility managers should assess their cybersecurity goals and determine if their current program meets those risk-based goals, or if an adjustment is needed. The B-C2M2 can be reapplied in the future to determine if the facility is still meeting its goals or making progress toward meeting them.

The authors made a number of key observations when analyzing results from the four pilot assessments. These observations might represent a large majority of facilities and buildings that employ automated building control systems and networks. However, because of the small sample size the authors could not draw any broadly representative conclusions.

All four of the pilot facilities had enterprise-level cybersecurity programs to protect their IT systems. These ranged from a well-documented program administered by a large IT department to a largely undocumented program administered by one IT person. None of the pilot sites had a well-documented cybersecurity program for its building control systems. Instead the sites conducted mostly undocumented, *ad hoc* cybersecurity activities to support building control system security. The more mature the enterprise-level cybersecurity program, the greater the time and attention were applied to building control system security, but not enough attention to warrant comprehensive documentation of the associated cybersecurity program.

At all of the four pilot sites, building control system engineers and IT representatives acknowledged that additional resources, including staff time, would need to be allocated to more thoroughly address cybersecurity issues for building control systems.

A striking feature at the four pilot sites was the lack of a structured cybersecurity risk assessment for the building control systems. At one site, the building control system engineers recognized the potential for cyber threats and had informally prioritized the allocation of resources to address those building control systems that were perceived to pose the greatest risks to safety, security, and operations. At the other end of the spectrum, there were sites where the risks of a cyberattack on the building control systems were not factored into decision making.

If cybersecurity activities for building control systems are not documented, the actions taken by building control system engineers to protect their systems will vary from individual to individual. Although some building control system engineers were doing a fine job in securing their systems at the pilot sites, the lack of documentation and succession planning raised serious continuity issues. If key individuals left their current positions (for any reason), the lack of documentation and succession planning would result in an immediate and appreciable drop in the maturity of an operational cybersecurity program.

At most of the pilot sites, there was a noted lack of formal coordination between enterprise IT security and building control system security. The most mature enterprise IT cybersecurity program provided a defensive architecture and other security controls that enhanced the security of the building control systems. The IT organization at that facility was actively engaging with the building control system engineers to assess and enhance the security of the building control systems. However, this level of engagement was only a recent development and was not yet covered by documented procedures.

Security monitoring on building control systems at all four pilot sites was enabled by products provided by the vendor of the automated control system. These products generally searched for performance outside of the limits set by the local building control system engineer. Control systems are sensitive to weather, software, computation errors, and host of other factors that can cause them to alarm. The level of fine-tuning of the alarm limits by the building control system engineers varied from site to site. At one site, monitoring alarms were carefully set to reduce false alarms and a prompt response to alarms was an expected part of the building control system engineers' duties. Responsibility for monitoring alarms was shared so that there was around the clock coverage to respond to alarms. At another site, alarm limits were not carefully set and the frequent false alarms often resulted in a delayed response or alarms being ignored if they appeared noncritical. In other cases, there was an insufficient number of building control system staff members to provide an around-the-clock alarm monitoring and response capability.

At all four sites, cybersecurity training and awareness programs for building control system engineers were limited. At the most mature site, building control system engineers received some cybersecurity training and had an elevated awareness of cybersecurity issues. There was evidence of informal training activities and independent cybersecurity study by the building security engineers. At another site, the building control system engineer had only a passing familiarity with cybersecurity issues and the enterprise-level IT representative was so overwhelmed in dealing with enterprise IT security issues that building control system security issues were not being considered.

Perhaps the most rewarding aspect of conducting the B-C2M2 assessment was a response heard several times at each site from the building control system engineers and IT personnel: "*I hadn't thought of that—that could be a problem. I should start paying attention to that issue…*"

If the only accomplishment derived from the approximately one hour spent performing a B-C2M2 assessment was a heightened awareness of building control system security issues, that by itself indicates it was an hour well spent.

Conclusions and Next Steps

The B-C2M2 was developed to provide an easy-to-use method for facility and building managers and staff to quickly evaluate the maturity of the cybersecurity program for their building control systems. Based on the C2M2 developed for use within the energy sector, full and Lite versions of the B-C2M2 are available. Results from a B-C2M2 assessment provide a way for facility managers, building system engineers, and IT personnel to estimate the maturity of their cybersecurity program, evaluate their cybersecurity program status against the risk of a successful cybersecurity attack, establish programmatic goals, and monitor progress in achieving those goals. In addition, as pilot testing demonstrated, the experience of applying the B-C2M2 will identify a number of issues that staff members have not previously considered and can easily address. Just bringing up these types of issues might by itself appreciably increase the maturity of the cybersecurity program supporting building control systems.

The development, testing, and application of the B-C2M2 are continuing. Information on user experiences and feedback will be used to shape the future development and deployment of the B-C2M2. Work is under way on user guidance products and reporting tools, to further assist building control system personnel in applying the B-C2M2 at their facility.

The B-C2M2 is not an isolated product. Complementary work is under way to build a DOE Buildings Cybersecurity Framework that is compatible with the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (NIST 2014). The NIST framework document provides a structure that organizations, regulators, and customers from different critical infrastructure sectors can use to create, guide, assess, or improve comprehensive cybersecurity programs. The DOE Buildings Cybersecurity Framework will streamline and focus the concepts introduced in the NIST framework to address cybersecurity issues for building control systems and smart connected equipment and assets. Guided by industry and stakeholder input, the DOE framework will capture new operational and risk management processes, security practices, and governance for the security of building control systems and smart assets. The DOE framework will recognize important optimization opportunities for energy efficiency as well as the need to mitigate increasingly complex cyber challenges.

The DOE Buildings Cybersecurity Framework will address the convergence and interconnection of IT and control systems in buildings and the challenges this creates in terms of organizational roles and responsibilities, new operational complexities, and security risks. The B-C2M2 will support the DOE framework by providing an easy-to-use method for assessing the maturity of cybersecurity programs, provide for goal setting, measure progress toward goals, and enhance cybersecurity situational awareness for buildings. Other tools and technologies will be offered to provide more in-depth assessment capabilities to those facilities and buildings that require it.

References

78 FR 11739-11744. February 19, 2013. “Executive Order 13636—Improving Critical Infrastructure Cybersecurity.” *Federal Register*, https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

Albion, L., M.C. Libicki, and A.A. Golay. 2014. *Markets for Cybercrime Tools and Stolen Data*. Santa Monica, CA: RAND National Security Research Division. file:///C:/Users/d39474/Documents/w16/Cyber%20Reference/RAND/RAND_RR610.pdf.

Clapper, J. 2015. "Statement for the Record: Worldwide Cyber Threats." Presented to the U.S. House Permanent Select Committee on Intelligence by James R. Clapper, Director of National Intelligence, September 10, 2015. http://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf.

DHS (US Department of Homeland Security). 2011. *Cross-Sector Roadmap for Cybersecurity of Control Systems*. Washington, DC: US Department of Homeland Security's National Cybersecurity Division. https://scadahacker.com/library/Documents/Roadmaps/Cross%20Sector%20Roadmap%20for%20Cybersecurity%20of%20Control%20Systems.pdf.

DOE (US Department of Energy). 2011. *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. Washington, DC: U.S. Department of Energy. http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

———. 2014. *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.1*. Washington, DC: US Department of Energy. http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf .

ICS-CERT (Industrial Control System Cyber Emergency Response Team). 2016. "Assessments." https://ics-cert.us-cert.gov/Assessments.

Interagency Security Committee. 2015. *Presidential Policy Directive 21, Implementation: An Interagency Security Committee White Paper*. Washington, DC: US Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf.

Mylrea, M. 2015. *Cyber Security and Optimization in Smart Autonomous Buildings*. Association for the Advancement of Artificial Intelligence Symposium. Palo Alto, CA: Stanford University. http://www.aaai.org/ocs/index.php/SSS/SSS15/paper/view/10339

NIST (US National Institute of Standards and Technology). 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1. Washington, DC: US Department of Commerce. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

White House. 2010. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington, DC: The White House. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.