Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

> *"The truth is rarely pure and never simple."*
>
> Oscar Wilde (1854–1900)
> Writer, poet, and playwright

Critical infrastructure such as power generation and distribution systems, telecommunications networks, pipelines and pipeline control networks, transportation control networks, financial networks, and government information and communications technology (ICT) have increasingly become the target of cyber-attacks. The impact and cost of these threats, as well as regulatory pressure to mitigate them, have created an impetus to secure these critical infrastructures. Managers have many controls and models at their disposal to help them secure infrastructure technology, including cybersecurity capability maturity models to enable measurement and communication of cybersecurity readiness to top management teams, regulators, and customers, thereby facilitating regulatory compliance, corporate responsibility, and improved brand quality. However, information and awareness is lacking about which models are most appropriate for a given situation and how they should be deployed.

This article examines relevant cybersecurity capability maturity models to identify the standards and controls available to providers of critical infrastructure in an effort to improve their level of security preparedness. These capability models are described and categorized by their relevance to different infrastructure domains, and then recommendations are provided on employing capability maturity models to measure and communicate readiness. This article will be relevant to regulators, critical infrastructure providers, and researchers.

Introduction

The critical infrastructures that make our way of life possible are increasingly vulnerable to cyber-attack. These critical infrastructures are defined as assets or systems required for the security and well being of citizens, including systems to produce and distribute water, electricity, and fuel, and communication networks (Public Safety Canada, 2009; Yusta et al., 2011; European Commission, 2013; U.S. Department of Homeland Security, 2013). Accordingly, disruption to one or more of these critical infrastructures usually incurs substantial human and financial cost, which is often the point of a cyber-attack and the reason such infrastructures are targeted by actors who may be motivated by profit or sociopolitical causes, among other motivations (Grau & Kennedy, 2014).

As the types of connectivity and volumes of data flow increase, the potential for cyber-attacks increases (Dupont, 2013) and brings greater focus on the security of critical infrastructures. In preparing their systems to withstand cyber-attacks, operators of critical infrastructure are faced with myriad controls and standards, and many of their implementations are incomplete or inconsistent, which further exacerbates the threat environment and provides a false sense of security (Chaplin & Akridge, 2005). To properly secure critical infrastructure and accurately report on its readiness to withstand cyber-threats, operators need a common measurement apparatus in addition to standard controls.

Providers of critical infrastructure have turned to cybersecurity capability maturity models to provide a framework for assessing and reporting cybersecurity

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

readiness. A capability maturity model improves the maturity and efficacy of controls employed to secure critical infrastructures. Such models delineate a sequence of maturity levels for a class of objects and represent an anticipated, desired, or typical evolution path of these objects shaped as discrete stages (Becker et al., 2009). This evolution should be sequential in nature and should have defined criteria for measurement (Wendler, 2012). A cybersecurity capability maturity model should be interpreted by subsector organizations of various types, structures, and sizes for the purpose of augmenting existing enterprise cybersecurity plans (U.S. Department of Energy, 2014). Cybersecurity capability maturity models have been developed for specific industry subsectors, but government implementation methods vary globally: public-private collaborations are the most common form of implementation in the United States and Canada, whereas regulatory schemas are more common in Europe and elsewhere (Yusta et al., 2011). And, as we will show in this article, the existing models tend to be descriptive, not prescriptive, in nature.

Given that cybersecurity is a global priority and a shared responsibility, there should be adequate motivation to develop more comprehensive critical infrastructure definitions and cybersecurity capability maturity models (Agresti, 2010). But, unfortunately, as we argue in this article, our toolkit of cybersecurity capability maturity models is itself insufficiently mature to address the full extent and magnitude of cyber-threats facing critical infrastructure today.

The purpose of this article is to examine current cybersecurity maturity models and evaluate their applicability to providers of interdependent critical infrastructures such as municipal governments. It contributes to practice by identifying a new category for assessing cybersecurity issues resulting from the interdependency of critical infrastructure. The article also highlights a gap in the existing cybersecurity literature relative to the adoption of capability maturity models by operators of interdependent critical infrastructures such as municipalities, which are often responsible for power, water, and emergency services, for example. By understanding this new category, researchers and practitioners alike will be better equipped to influence adoption of capability maturity models in securing and reporting on critical infrastructure cybersecurity readiness.

The article is organized as follows. First, we examine definitions of critical infrastructure and related regulatory frameworks in the European Union, the United States, and Canada. Next, we outline common threats to critical infrastructure. Then, we review and categorize the characteristics of current cybersecurity capability maturity models and their applicability to critical infrastructure operators, particularly those who have interdependent systems, such as municipalities. Finally, we offer managerial recommendations for employing cybersecurity capability models, identify gaps in the literature, and highlight areas for further study.

What is Critical Infrastructure?

Critical infrastructure includes any element of a system that is required to maintain societal function, maintain health and physical security, and ensure social and economic welfare (Yusta et al., 2011). Widely accepted examples of critical infrastructure are energy and utilities, financial systems, food, transportation, government, information and communications technology, health, and water purification and distribution. However, these elements do not operate in isolation today. Increasingly, connectivity and interdependencies between such systems increase the complexity of managing critical infrastructure and modelling the risks of cybersecurity threats (Rahman et al., 2011; Xioa-Juan & Li-Zhen, 2010). Indeed, Xiao-Juan and Li-Zhen (2010) state that "the computerization and automation of critical infrastructures have led to pervasive cyber interdependencies". And, Rahman, Martí, and Srivastava (2011) discuss the difficulty in assessing the effects that failures in communications networks may have on municipal infrastructures such as hospitals and emergency services. They further state that cyber-interdependencies comprise a fundamental class of interdependency in critical infrastructure networks.

To help cope with the security risks associated with the complexity and interdependencies within various critical infrastructure systems, standards bodies and federal agencies in at least twelve countries or regions have defined criteria for security standards as well as implementation methods (Yusta et al., 2011). For example, the European Union (EU) has moved towards a legislated critical infrastructure regimen through the European Programme for Critical Infrastructure Protection (EPCIP), and the United States has adopted a cooperative model between the Department of Homeland Security and industry with the National Infrastructure and Protection Plans of 2009 and 2013. In Canada and the United Kingdom, cooperative frameworks are also in place through the National Strategy for Critical Infrastructure and the Centre for the Protection of National

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

Infrastructure, respectively (Table 1). As a EU member, the United Kingdom has authored its own framework as recommended in the EPCIP.

In these four examples of federal government regulatory frameworks, only the EPCIP legislates a response from government and industry operators of critical infrastructure. In the EPCIP, obligations on EU nations are specified and supports are made available for EPCIP adoption by member states. In each of the remaining three examples – Canada, the United Kingdom, and the United States – a cooperative framework between government and operators is employed to foster communication of best practices for critical infrastructure and threats against it. These frameworks rely on adoption by operators rather than mandating compliance.

The literature on critical infrastructure emphasizes the importance and difficulty of assessing the cybersecurity readiness of interdependent networks. Each of the four frameworks in Table 1 recognizes interdependencies of critical infrastructure based on geographic considerations and specifies that collaboration is required to ensure an adequate response to critical infrastructure failures. However, when defined critical infrastructure such as water and power distribution, traffic control, emergency services, and the like are considered, the linkage between interdependent critical infrastructure and municipal governments as operators of multi-faceted critical infrastructure becomes apparent. Municipal governments require a framework suitable for evaluating and reporting the readiness of their interdependent critical infrastructures.

Threats to Critical Infrastructure

As the complexity and interdependencies of critical infrastructure increase, providers of critical infrastructure must cope with increasing vulnerability of their management systems to cyber-threats. As outlined in the *US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Office of the US President, 2003), three effects may constitute vulnerability on a system:

1. *Direct infrastructure effect*: Cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function.

2. *Indirect infrastructure effect:* Cascading disruption and financial consequences for government, society, and economy through public and private sector reactions to an attack.

3. *Exploitation of infrastructure:* Exploitation of elements of a particular infrastructure to disrupt or destroy another target.

The increasing complexity of such system vulnerabilities, and the complexity of the threats themselves, necessitates cooperation between the industry and the government. These existing and emerging trends lead to a requirement for the consistent implementation of cybersecurity by industry stakeholders, key infrastructure providers, and government in order to protect critical infrastructure vital to financial, commercial, and social well being.

Table 1. Examples of cybersecurity regulations and frameworks

Region	Regulation	Model
European Union	European Programme for Critical Infrastructure Protection (EPCIP) tinyurl.com/nwgajk2	Regulation
Canada	National Strategy for Critical Infrastructure (NSCI) tinyurl.com/qcvryqv	Cooperative Framework
United Kingdom	Centre for the Protection of National Infrastructure (CPNI) tinyurl.com/kuplrq5	Cooperative Framework
United States	National Infrastructure and Protection Plan (NIPP 2013) tinyurl.com/n5ppvhs	Cooperative Framework

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

Cybersecurity Capability Maturity Models

Increased awareness of threats to constituents, and compliance frameworks at the federal government and industry levels, have created a need to assess and report on the readiness of the critical infrastructure provider using cybersecurity capability maturity models. With their roots in the software industry, capability maturity models originally represented a path of improvements recommended for organizations that want to increase their software process capability (Wendler, 2012). Typically, a capability maturity model has two components: i) a means of measuring and describing the development of an object in a sequential manner showing hierarchical progression, and ii) criteria for measuring the capabilities of the objects such as conditions, processes, or application targets. Together, these components provide a sequence of maturity levels for a class of objects. In other words, a capability maturity model represents an anticipated, desired, or typical evolution path of these objects shaped as discrete stages (Becker et al., 2009). They allow an organization to examine its capabilities sequentially in multiple dimensions and show hierarchical progression, thereby generating yardsticks representing defined maturity levels.

The concept of capability maturity models has been extended to the domain of cybersecurity and can be applied to the protection of critical infrastructure. In lieu of simple checklists, managers now have well-defined criteria against which to measure the maturity of their preparedness against cyber-threats (Debreceny, 2006; Lahrmann et al., 2011; Siponen, 2002), with models shifting from early examples such as the International Organization for Standardization's Systems Security Engineering Capability Maturity Model (SSE-CMM), Citigroup's Information Security Evaluation Model (CITI-ISEM) and Computer Emergency Response Team / CSO Online at Carnegie Mellon University (CERT/CSO) around the turn of the century to modern initiatives such as the current International Organization for Standardization (ISO/IEC) standards, the National Institute of Standards and Technology (NIST) Cybersecurity framework, the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2), and the U.S. Department of Homeland Security's NICE-CMM released in 2014. These modern cybersecurity capability maturity models provide the stages for an evolutionary path to developing policies and processes for the security and reporting of cybersecurity readiness of critical infrastructure.

The U.S. Department of Energy's C2M2, as well as the companion capability maturity models ES-C2M2 and ONG-C2M2, provides a maturity model and evaluation tool to facilitate cybersecurity readiness for operators of energy production and distribution networks. However, this tool is specific to the energy sector, which limits its applicability.

The U.S. Department of Homeland Security's NICE-CMM and the Software Engineering Institute at Carnegie Mellon University focus on workforce development, process maturity, and operational resilience practices to aid organizations in cybersecurity readiness. They do not offer specific cybersecurity best practices, however. Additional frameworks must be employed in conjunction with these models.

The ISO standards provide guidance covering the range of device certification (ISO/IEC 15408), information security management systems (ISO/IEC 27001), and software security engineering processes (ISO/IEC 21827 or SSE-CMM). Used together, these standards provide a complementary regimen for an organization's cybersecurity readiness; however, navigating the many standards is complicated and has time and cost implications.

The NIST cybersecurity framework provides a set of activities to aid organizations in developing individual readiness profiles. Although this framework is robust, it relies on operators to voluntarily develop individual profiles for their organizations.

The models described here – and summarized in Table 2 – provide guidance for organizations to prepare cybersecurity readiness plans, but aside from the ISO standards, they offer only high-level advice, and many apply only to specific industry verticals. The ISO standards, while offering more specific advice, are complicated to implement and do not specifically address our operators of interdependent critical infrastructure such as municipal governments. Thus, a model specific to this category of operator is required to adequately prepare for the possible cyber-attacks on municipal critical infrastructure.

Adoption of Cybersecurity Capability Maturity Models

Our review of the available cybersecurity capability maturity models shows that they are complicated to implement, have time and cost implications, and an

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

Table 2. Cybersecurity capability maturity models for critical infrastructure

Model	Publisher	Purpose
C2M2 (tinyurl.com/kvtuacm)	US Dept. of Energy	Assessment of cybersecurity capabilities for any organization comprised of a maturity model and evaluation tool
ES-C2M2 (tinyurl.com/pe62edg)	US Dept. of Energy	C2M2 tailored to energy subsector
ONG-C2M2 (tinyurl.com/mx3qzyk)	US Dept. of Energy	C2M2 tailored to the oil and natural gas subsector
NICE-CMM (tinyurl.com/m3224qv)	US Dept. of Homeland Security	Defines three areas: process and analytics, integrated governance, skilled practitioners and technology for workforce development
CERT-RMM (tinyurl.com/mp85m7y)	CERT/SEI	Defines organizational practices for operational resilience, security, and business continuity
ISO/IEC 15408 (tinyurl.com/mvw3dxl)	ISO	Criteria for computer security certification
ISO/IEC 27001 (tinyurl.com/kh2t2uo)	ISO	Information Security Management System (ISMS) specification
ISO/IEC 21827 SSE-CMM (tinyurl.com/obfeup3)	ISO	Evaluation of software security engineering processes
NIST Cybersecurity Framework (tinyurl.com/kugdfug)	NIST	Framework for improving federal critical infrastructure through a set of activities designed to develop individual profiles for operators

organization's processes may need to be refined during implementation. However, three of the regulatory frameworks in Table 1 rely on their voluntary adoption by operators of critical infrastructure, leading us to ponder how adoption of these models can be fostered effectively in an unlegislated environment.

Rogers (1983) explains that large organizations such as municipalities can be seen as laggards in his diffusion of innovation adopter categories. Diffusion of innovation theory also identifies five factors that impact adoption: relative advantage (i.e., the value that the innovation provides over the current method); compatibility (i.e., how easily the innovation incorporates into the current routine), simplicity (i.e., whether the innovation is difficult to use); trialability (i.e., how easy it is to try the innovation without commitment); and observability (i.e., how visible the innovation is in a community of the adopter's peers). Considering these five factors and the adopter categories, several categories of motivators and capabilities must be addressed to prompt adoption of cybersecurity capability maturity models by a given operator.

For example, increased observability of vulnerabilities by a critical-infrastructure operator peer group can inform executives on the will and direction of their association and may form the impetus for adoption by the industry. Similarly, enhancing the regulatory frameworks shown in Table 1 or brand damage resulting from exploitation can inform executives on their obligations to securing critical infrastructure and form the impetus for adoption. The availability of applicable capability maturity models for the operator and competent staff may address the factors of simplicity and trialability. We contend that applying diffusion of innovation theory to assess adoption methods will help build a cybersecurity capability maturity model for operators of interdependent critical infrastructure such as municipal governments.

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

Conclusion

Modern society has become increasingly dependent on the computers and systems that control our critical infrastructure and in doing so have created a scenario whereby a cyber-attack can have serious impacts on our way of life. In the case of municipal governments that operate a network of interdependent systems, the impacts of such a cyber-attack could be far reaching. The unique properties and criticality of these entities constitutes a new category of critical infrastructure provider that warrants study.

Our review of the current cybersecurity capability maturity models highlighted that, although many models exist, none are specifically crafted to address the scenario of an operator of multiple interdependent systems. Rather, they are focused on federal infrastructures or specific industry sub-sectors, and are all at a high level. The absence of a cybersecurity capability maturity model for municipal governments provides an opportunity for further research to industry experts and researchers of cybersecurity capability maturity models.

Although the regulatory frameworks shown in Table 1 provide clear definitions of critical infrastructure and the need to secure them, they lacked a focus on adoption of cybersecurity capability maturity models, relying on operators to define and adopt best practices. We postulate that Rogers' (1983) diffusion of innovation theory can be applied when building and facilitating industry adoption of a cybersecurity capability maturity model for municipal operators of critical infrastructure, and this topic may be worthy of further study.

This article contributes to the literature in two ways.

1. It identifies a new category for operators of *interdependent networks of critical infrastructure*, highlighting the need for a cybersecurity capability maturity model for operators such as municipal governments.

2. It highlights a gap in the literature relative to the adoption of cybersecurity capability maturity models, particularly at the municipal level, providing an opportunity for further research.

In summary, this article discussed critical infrastructure, cybersecurity capability maturity models, and factors affecting their adoption. We found that there is an opportunity to develop a cybersecurity capability maturity model that better addresses the unique properties of operators of interdependent critical infrastructures. Researchers may seize the opportunities for further study on cybersecurity capability maturity models and their adoption. Operators should consider Rogers' five-factors when reviewing their plans for augmenting their cybersecurity readiness.

About the Authors

Walter Miron is a Director of Technology Strategy at TELUS Communications, where he is responsible for the evolution of their packet and optical networks. He has over 20 years of experience in enterprise and service provider networking conducting technology selection and service development projects. Walter is a member of the research program committee of the SAVI project, the Heavy Reading Global Ethernet Executive Council, and the ATOPs SDN/nFV Working Group. He is also Chair of the Venus Cybersecurity Corporation and a board member of the Centre of Excellence for Next Generation Networking (CENGN) in Ottawa, Canada. Walter is currently a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada.

Kevin Muita is a graduate student in the Technology Innovation Management program at Carleton University in Ottawa, Canada. He has a Bachelor's degree in Technology from Africa Nazarene University in Nairobi, Kenya. He has co-founded two technology startups: a network consultancy company and a systems installation and maintenance company. He has experience in logistics and supply chain management, having managed a Coca-Cola distribution network in Kenya, overseeing a successful 300% increase in sales volume, operations, and service delivery.

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

References

Agresti, W. 2010.The Four Forces Shaping Cybersecurity. *Computer,* 43(2): 101-104. http://dx.doi.org/10.1109/MC.2010.53

Becker, J., Knackstedt, R., & Pöppelbuß, J. 2009. Developing Maturity Models for IT Management. *Business & Information Systems Engineering,* 1(3): 213-222. http://dx.doi.org/10.1007/s12599-009-0044-5

Chaplin, D. A., & Akridge, S. 2005. How Can Security Be Measured? *Information Systems Control Journal,* 2.

Debreceny, R. S. 2006. Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences:* 196c. http://dx.doi.org/10.1109/HICSS.2006.407

Dupont, B. 2013. Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review,* 3(7): 6-11. http://timreview.ca/article/700

European Commission. 2013. Critical Infrastructure. European Commission, Home Affairs. July 20, 2014: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

Grau, D., & Kennedy, C. 2014. TIM Lecture Series – The Business of Cybersecurity. *Technology Innovation Management Review,* 4(4): 53-57. http://timreview.ca/article/785

Lahrmann, G., Marx, F., Mettler, T., Winter, R., & Wortmann, F. 2011. Inductive Design of Maturity Models: Applying the Rasch Algorithm for Design Science Research. In H. Jain, A. P. Sinha, & P. Vitharana (Eds.), *Service-Oriented Perspectives in Design Science Research:* 176–191. Berlin: Springer. http//dx.doi.org/10.1007/978-3-642-20633-7_13

Office of the US President. 2003. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Washington, DC: The White House. http://www.dhs.gov/national-strategy-physical-protection-critical-infrastructure-and-key-assets

Public Safety Canada. 2009. *National Strategy for Critical Infrastructure.* Ottawa: Government of Canada. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx

Rahman, H. A., Martí, J. R., & Srivastava, K. D. 2011. A Hybrid Systems Model to Simulate Cyber Interdependencies between Critical Infrastructures. *International Journal of Critical Infrastructures,* 7(4): 265–288. http://dx.doi.org/10.1504/IJCIS.2011.045056

Rogers, E. M. 1983. *Diffusion of Innovations.* New York: Free Press.

Siponen, M. 2002. Towards Maturity of Information Security Maturity Criteria: Six Lessons Learned from Software Maturity Criteria. *Information Management & Computer Security,* 10(5): 210–224. http://dx.doi.org/10.1108/09685220210446560

U.S. Department of Energy. 2014. *Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2 v1.1).* Washington, DC: U.S. Department of Energy. http://energy.gov/oe/downloads/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-february-2014

U.S. Department of Homeland Security. 2013. What Is Critical Infrastructure? Washington, DC: U.S. Department of Homeland Security. July 20, 2014: http://www.dhs.gov/what-critical-infrastructure

Wendler, R. 2012. The Maturity of Maturity Model Research: A Systematic Mapping Study. *Information and Software Technology,* 54(12): 1317-1339. http://dx.doi.org/10.1016/j.infsof.2012.07.007

Xiao-Juan, L., & Li-Zhen, H. 2010. Vulnerability and Interdependency of Critical Infrastructure: A Review. *Third International Conference on Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA):* 1–5. http://dx.doi.org/10.1109/INFRA.2010.5679237

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. 2011. Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art. *Energy Policy,* 39(10): 6100–6119. http://dx.doi.org/10.1016/j.enpol.2011.07.010

Citation: Miron, W., & Muita, K. 2014. Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. *Technology Innovation Management Review,* 4(10): 33–39. http://timreview.ca/article/837

Keywords: cybersecurity, critical infrastructure, capability maturity models, municipalities, standards, compliance, protection, regulation, framework, adoption