Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects

Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge

> *"The challenge in the digital economy is that no chain is stronger than its weakest link."*
>
> Christian Wernberg-Tougaard
> Global Lead for Social Welfare & Human Services
> at Oracle Corporation

Many systems that comprise our critical infrastructures – including electricity, transportation, healthcare, and financial systems – are designed and deployed as information technology (IT) projects using project management practices. IT projects provide a one-time opportunity to securely "design in" cybersecurity to the IT components of critical infrastructures. The project management maturity models used by organizations today to assess the quality and rigour of IT project management practices do not explicitly consider cybersecurity. This article makes three contributions to address this gap. First, it develops the argument that cybersecurity can and should be a concern of IT project managers and assessed in the same way as other project management capabilities. Second, it examines three widely used cybersecurity maturity models – i) the National Institute of Science and Technology (NIST) framework for improving critical infrastructure cybersecurity, ii) the United States Department of Energy's Cybersecurity Capability Maturity Model (C2M2), and iii) the CERT Resilience Management Model (CERT RMM) from the Carnegie Mellon Software Engineering Institute – to identify six cybersecurity themes that are salient to IT project management. Third, it proposes a set of cybersecurity extensions to PjM3, a widely-deployed project management maturity model. The extensions take the form of a five-level cybersecurity capability perspective that augments the seven standard perspectives of the PjM3 by explicitly assessing project management capabilities that impact the six themes where IT project management and cybersecurity intersect. This article will be relevant to IT project managers, the top management teams of organizations that design and deploy IT systems for critical infrastructures, and managers at organizations that provide and maintain critical infrastructures.

Introduction

Cybersecurity attacks on information technology (IT) systems are becoming increasingly frequent and sophisticated (Bailey et al., 2014). *Critical infrastructures* – the assets essential for the functioning of a society and economy (Public Safety Canada, 2009) such as power generation and distribution, transportation systems, healthcare services, and financial systems – are increasingly reliant on networked IT systems (Rahman et al., 2011; Xiao-Juan & Li-Zhen, 2010). Securing these interconnected IT systems from cyber-attack is thus of growing concern to many stakeholders (Merkow & Raghavan, 2012). Security experts argue that security should be "designed in" to critical systems upfront, rather than retrofitted later (Hughes & Cybenko, 2013; McGraw, 2006; Pfleeger et al., 2015).

Cybersecurity capability maturity models (e.g., Caralli et al., 2010; NIST, 2014; U.S. Department of Energy, 2014) are one approach used by organizations to assess capability to defend against cyberattacks, benchmark cybersecurity capability against others, and identify cybersecurity capabilities to improve (Miron & Muita, 2014). Like the maturity models in other specialized domains, cybersecurity capability maturity models help organizations to measure their current processes against established industry standards. However, current cybersecurity capability maturity models overwhelmingly focus on evaluating how organizations protect existing systems (i.e., processes to *maintain* cybersecurity) rather than evaluating how organizations securely develop and deploy new secure information systems (i.e., processes to *create* cybersecurity).

New IT systems are typically developed and deployed as *IT projects* (Phillips, 2010), which are managed using project management practices (PMI, 2013a). IT projects provide a one-time opportunity to "design in" cybersecurity to the new IT systems deployed within critical infrastructures. Although the project management domain has its own maturity models (e.g., Sowden et al. 2013; PMI, 2013b), the project management models in use today do not explicitly address cybersecurity. For providers of critical infrastructures and their stakeholders, this is both a gap and an opportunity.

This article makes three contributions to the theory and practice of securing critical infrastructures. First, it develops the argument that cybersecurity can and should be a concern of the IT project managers and project sponsors of critical infrastructure IT projects, and that project management maturity models could be extended to assess cybersecurity capability in the same way that these models assess other capability domains. Second, it identifies six cybersecurity themes that are salient to IT project management. It accomplishes this by selecting three cybersecurity capability maturity models, examining the content and areas of commonality, and identifying those aspects that overlap with the scope of IT project management or are likely to be impacted by project management decisions and activities. The themes therefore reflect both building secure systems and also building systems in secure way. The three models examined are: i) the National Institute of Science and Technology (NIST) framework for improving critical infrastructure cybersecurity, ii) the United States Department of Energy's Cybersecurity Capability Maturity Model (C2M2), and iii) the CERT Resilience Management Model (CERT RMM). Third, it selects a project management maturity model – the PjM3 – and proposes a new five-level cybersecurity capability perspective that augments the seven capability perspectives of the standard model. Bringing together cybersecurity capability maturity models and the PjM3 project management maturity model provides critical infrastructure organizations with the means to evaluate capability in upstream "cybersecurity creation". This approach will be especially useful for organizations that highly value security and concurrently employ cybersecurity capability maturity models to evaluate capability in downstream "cybersecurity maintenance".

The body of this article is structured as four sections. The next three sections each develop one of the article's three contributions and the fourth section concludes.

Securing the IT Project

IT systems within critical infrastructures typically originate as IT projects (Phillips, 2010). Unlike operations, which are continuous and on-going, projects have a specific set of objectives and well-defined and finite time boundaries (Kerzner, 2013). IT development and deployment activities are typically managed using project management tools and techniques, such as those of the Project Management Body of Knowledge (PMBOK; PMI, 2013a), and an IT project management process with well-defined stages and gates between stages (Phillips, 2010).

Decisions and activities within an IT project are likely to have a lasting impact on cybersecurity. Procurement and supply chain management are one example. Outsourced design services, purchase of commercial off-the-shelf (COTS) software, and the adoption of open source software components are all potential sources of vulnerabilities that are difficult to detect and correct later (Ellison et al., 2010). Quality management is a second example. Defects in design, deployment, or provisioning during the IT project could be exploitable until detected and corrected – potentially throughout the active lifecycle of the IT system. The security of the project office and the project infrastructure is also of lasting impact. The tools and processes used for project work, document management, and communication within the project team are all components of information security and integrity. For example, project artifacts thought to be private could be a goldmine to attackers for future social engineering attacks. Thus, IT projects provide a one-time opportunity to securely "design in" cybersecurity to the new IT systems deployed within critical infrastructures.

Capability maturity models approach an activity as a process and formally compare the characteristics of the process in use against the characteristics of an "ideal" process (Humphrey, 1988). This approach originated in software engineering and has been widely applied in many specialized domains, including cybersecurity (Miron & Muita, 2014), capacity to leverage open source software (Carbone, 2007), and enterprise-readiness of open source software projects (Golden, 2008). Project management maturity models are the subset of capability maturity models that focus specifically on project management capabilities. A body of empirical evidence associates the use of project management standards, processes, and maturity models with positive project outcomes (Brookes, 2009; Milosevic & Patanakul, 2005).

The two most developed and widely deployed project management maturity models are:

1. PjM3, the project management component of the Portfolio, Programme, and Project Management Maturity Model (P3M3), maintained by a public–private partnership with the United Kingdom government (Sowden et al., 2013)

2. OPM3, the Organizational Project Management Maturity Model, developed and maintained by the Project Management Institute (PMI, 2013b)

In addition, there are many derivatives of both base models. For example, the PRINCE2 Maturity Model is a specialized derivative of the P3M3 that is specifically aligned with the PRINCE2 (Projects IN Controlled Environments, version 2) project management methodology (Office of Government Commerce, 2009).

Both of these models and their various derivatives address the management of project risks, but none explicitly address cybersecurity. Nonetheless, cybersecurity capability could be assessed at the same time and in the same way as other areas of concern within the scope of project management.

The remainder of this article focuses exclusively on the PjM3 project management capability maturity model. There are three reasons for selecting the PjM3 rather than a different model. First, the PjM3 is the most widely used model internationally (Young et al., 2011). Second, the PjM3 provides a discrete five-level score in seven perspectives (Sowden et al., 2013); discrete and modular models are more easily extensible for our purposes than, for example, the continuous scores of the OPM3. Third, the PjM3 is not explicitly connected with any particular project management framework or process (Sowden et al., 2013); it is thus more widely applicable than specialized models such as PRINCE2. Nonetheless, much of what follows about the PjM3 could be readily adapted to other project management models by repeating the steps described here.

The PjM3 is the project management component of the P3M3 – a broader maturity model that also addresses portfolio management and program management. The P3M3 was developed in 2006 by the Office of Government Commerce in the United Kingdom (OGC, 2006) and was most recently updated in 2013 by Axelos, a private–public partnership with the United Kingdom government (Sowden et al., 2013). It originated as an enhancement to OGC's Project Management Maturity Model, which had been adapted from the original Capability Maturity Model (CMM) developed by the Software Engineering Institute (SEI) in the United States (Humphrey, 1988). P3M3 has been adopted in both government and private organizations. For example, the Australian Department of Finance and Deregulation mandated P3M3 as the common methodology to evaluate Australian government agencies and assess their organizational capability to commission, manage, and realize benefits from ICT-enabled investments (Young et al., 2011).

The PjM3 assesses capability within seven process perspectives (Sowden et al., 2013): i) management control, ii) benefits management, iii) financial management, iv) stakeholder engagement, v) risk management, vi) organizational governance, and vii) resource management. Similar to other process maturity models, each perspective is independently assessed at one of five levels: awareness of process (level 1), repeatable process (level 2), defined process (level 3), managed process (level 4), and optimized process (level 5). Each level and each process perspective has embedded attributes. *Generic attributes* relate to all process perspectives at a maturity level. *Specific attributes* relate only to a particular process perspective. Thus the PjM3 is potentially extensible with new perspectives that employ the same structure and five-level measurement scale, and provide specific attributes for each maturity level.

Cybersecurity Capabilities

There is an extensive body of prior work on cybersecurity and on critical infrastructure that can inform a cybersecurity perspective on IT project management. Miron and Muita (2014) previously identified nine published cybersecurity capability maturity models for critical infrastructures. These nine models were published by five different organizations, with a variety of stated purposes. We employed the following steps to select three models for further examination. First, we scored each of the models identified by Miron and Muita (2014) in five areas: i) maturity and stability of authoring organizations; ii) experience in maturity modelling of authoring organizations; iii) the accessibility of detailed documentation; iv) publishing in the public domain or under open licenses; v) sufficient prescription of framework. Second, we employed three selection criteria: i) high scores in the five areas, ii) no more than one model from any one publisher, and iii) where two models received similar scores, we favoured the more general model or base model over a specialized or derivative model. This selection process was intended to select on both quality and diversity.

The following three cybersecurity capability maturity models were selected for further analysis:

1. The Cybersecurity Capability Maturity Model (C2M2) published by the United States Department of Energy (2014). The first C2M2 model was introduced in 2012, focused specifically on the energy subsector (ES-C2M2). It was updated most recently to version 1.1 in February 2014, and two new variants were launched: a basic sector-neutral version (C2M2; the version used here), and a version tailored to the oil and natural gas subsector (ONG-C2M2). Development was led by the United States Department of Energy (DoE) in partnership with the United States Department of Homeland Security (DHS), and in collaboration with public and private sector experts. C2M2 is structured as ten domains, each comprising a set of cybersecurity practices – the activities that an organization can perform to establish and grow capability in the domain.

2. The NIST Cybersecurity Framework from the National Institute of Science and Technology (NIST, 2014). The NIST Cybersecurity Framework was developed in response to a February 2013 executive order from the United States President to "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encouraged efficiency, innovation, and economic prosperity" (The President, 2013). It identifies a set of general principles and best practices to guide organizations to develop their own individual readiness profiles.

3. The CERT Resilience Management Model (CERT-RMM) from the Software Engineering Institute (SEI) at Carnegie Mellon University (Caralli et al. 2010). CERT-RMM was the first security model to adopt a capability maturity perspective. Beginning with the first drafts circulated in 2008, and now at version 1.1 (2010), the CERT-RMM was developed as the foundation for a process improvement approach to operational resilience management. It identifies organizational practices necessary to manage operational resilience and to respond to stress with mature and predictable performance.

Table 1 provides a summary of the content and main concerns of each of the three cybersecurity models. There are commonalities among all three models, concerns that are prominent in two of the three models, and unique concerns that are found in one model only.

Next, we systematically identified the cybersecurity concerns from Table 1 that are most salient to IT project management. We eliminated concerns that we deemed as purely operational and retained those concerns that either i) overlap with the scope of IT project management or ii) are likely to be impacted by project management decisions and activities. Finally, we grouped the remaining concerns into broad thematic areas, identifying six project-applicable cybersecurity themes:

1. Project environment security

2. Workforce security knowledge

3. Business continuity planning

4. Secure project supply chain

5. Project deliverable security

6. Project deliverable resiliency

These six themes provide a potential basis for a cybersecurity perspective on project management capability maturity.

Cybersecurity Extensions to the PjM3

To identify the specific attributes of a PjM3 cybersecurity perspective, we re-interpreted the six themes at each of the five levels of generic process-maturity attributes. By employing the same structure and measurement scale, we ensure that the new cybersecurity perspective is fully compatible with the seven standard perspectives of the PjM3, and can be assessed at the same time and in the same way as the standard perspectives.

Table 1. Content and main concerns of the C2M2, CERT-RMM, and NIST frameworks.

U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2)	Software Engineering Institute Cyber Risk and Resilience Management (CERT-RMM)	U.S. Department of Commerce NIST Framework for Improving Critical Infrastructure Cybersecurity
• Risk Management • Asset, Change, and Configuration Management • Identity and Access Management • Threat and Vulnerability Management • Situational Awareness • Information Sharing and Communication • Event and Incident Response, Continuity of Operations • Supply Chain and External Dependencies Management • Workforce Management • Cybersecurity Program Management	• Resilience Requirements Development • Resilience Requirements Management • Asset Definition and Management • Controls Management • Resilient Technical Solution Engineering • Service Continuity • External Dependency Management • Access Management • Identity Management • Incident Management and Control • Vulnerability Analysis and Resolution • Environmental Control • Knowledge and Information Management • People Management • Technology Management • Monitoring • Organizational Process Definition • Organizational Process Focus • Measurement and Analysis	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology • Anomalies and Events • Security Continuous Monitoring • Detection Processes • Response Planning • Response Communications • Analysis • Mitigation • Response Improvements • Recovery Planning • Recovery Improvements • Recovery Communications

The specific attributes at each of the five maturity levels, are provided in the following five subsections.

Level 1: Awareness

1. There are no cybersecurity training or skills requirements for any project team members.

2. There is no project role responsible for cybersecurity.

3. There is no access or identity control performed on system environments used by the project team.

4. There are no cybersecurity requirements maintained for projects.

5. Project cybersecurity processes such as Statements of Sensitivity (SoS), Threat Risk Assessment (TRA), and Privacy Impact Assessments (PIA) are not performed or are performed in an inconsistent, ad hoc manner.

6. Secure software development practices (e.g., code scans, penetration testing, OWASP) are neither planned nor performed.

7. Projects do not subscribe to organizational procurement standards or processes.

Level 2: Repeatable

1. Some team members have cybersecurity skills, but they are applied inconsistently throughout the team.

2. Project documentation is created, but there are no processes to maintain or control project documents or code.

3. Each project is responsible for ensuring appropriate identity and access management of project system environments.

4. Cybersecurity requirements are developed in an inconsistent and ad hoc manner.

5. Project cybersecurity processes (i.e., SoS, PIA, TRA, etc.) are employed in an inconsistent and ad hoc manner.

6. Secure software development practices (e.g., code scans, penetration testing, OWASP) are employed in an inconsistent manner across projects.

7. Business Continuity Plans are inconsistently employed by projects and rarely maintained.

Level 3: Defined

1. Cybersecurity skills are included in the job descriptions of key design, development, and testing roles.

2. Security screening of project resources is performed.

3. Project documentation and code is actively maintained in a secure repository.

4. A project role is identified as responsible for the cybersecurity of project deliverable(s).

5. There are defined processes for access and identity control of all system environments used by the project team.

6. Enterprise cybersecurity requirements are defined at the organizational level and are mandatory for all IT projects.

7. Checklists containing the details of all project cybersecurity processes (i.e., SoS, PIA, TRA, etc.) are available to all project team members.

8. Project standards for secure software development are defined and available to all team members.

9. Project standards for secure management of documentation and code exist and are available to all project team members.

10. Corporate procurement processes are employed by projects and all transactions are auditable.

11. Business Continuity Plan templates are made available to all project team members.

Level 4: Managed

1. Key design, development, and testing resources hold verifiable cybersecurity skills credentials.

2. Access and identity management configurations of project systems environments are consistently audited to ensure environment security and integrity.

3. All requirements documents are reviewed by an enterprise cybersecurity architect.

4. Phase containment exists to ensure that all project cybersecurity processes and standards (i.e., SoS, PIA, TRA, secure software development, Business Continuity Plans, etc.) are appropriately employed by each project and are of appropriate quality.

5. Projects only use qualified vendors who are, among other things, evaluated for security risk.

Level 5: Optimizing

1. Resources for improving cybersecurity skills that pertain to project work are made readily available to the entire project team.

2. A corporate Cybersecurity Centre of Excellence exists to continually improve the cybersecurity capability of project teams.

3. Corporate standards for project cybersecurity processes are continuously improved and actively communicated.

4. Corporate practices for secure software development are continuously improved and actively communicated.

5. Projects actively use their experience to contribute to corporate cybersecurity knowledge.

6. Enterprise cybersecurity requirements are continuously reviewed and improved by a Corporate Cybersecurity Centre of Excellence.

7. An enterprise security architect is required to sign-off on all major project deliverables.

8. Project documentation and code are maintained in a secure repository with strict version control.

9. All project documentation and code artifacts have only one copy, which is maintained in a secure repository.

10. Qualified vendors are continuously evaluated for security risk.

The cybersecurity perspective on project management capability maturity demonstrates the potential relationship between IT project management and cybersecurity of critical infrastructures. Much of the existing work on securing critical infrastructures, including the various cybersecurity maturity models, has emphasized ongoing operations. However, we suggest that an emphasis on operations addresses only half of the cybersecurity challenge, and we argue that the IT projects that design and deploy new IT systems also require attention. Cybersecurity extensions to project management maturity models – such as the PjM3 cybersecurity perspective proposed above – address the introduction of new systems in a way that will be familiar to experienced project managers and project sponsors.

Conclusion

As cybersecurity becomes an increasing area of concern for critical infrastructure providers, governments, and private enterprise, it warrants greater attention from IT project managers, project management offices, and project sponsors. We have argued that IT projects provide an opportunity to securely "design in" cybersecurity to the information systems components of critical infrastructures; thus, cybersecurity can and should be a main concern of IT project managers. A cybersecurity perspective on project management maturity addresses this opportunity in a form that is familiar to project practitioners.

Although this work is presented here at an early stage and has not yet been proven in the field, we sincerely hope that it sparks a dialogue between IT project practitioners, cybersecurity professionals, and providers of critical infrastructures on how to more effectively secure the systems that are essential for the functioning of our society and our economy.

Successful implementation will require action by multiple groups. We call upon IT project managers and project staff to try out these ideas in the field – beginning with informal self-assessments of cybersecurity maturity and followed by action plans to raise scores – and then to report back on their experiences. We call upon critical infrastructure project sponsors to provide IT project managers and project teams with the authority, incentives, training, and resources to "design in" cybersecurity to IT projects and assess the maturity of those efforts. We call upon researchers to empirically test the efficacy of these ideas, particularly the relationships between IT project cybersecurity attributes and high-impact outcomes, including traditional project outcomes, security outcomes, and operational outcomes. If evidence from the field shows this approach to be effective, adoption on a larger scale will require actions from project management organizations to incorporate cybersecurity more formally into the Pj3M and other project management standards. This formalization would open up new revenue opportunities for providers of training services, for providers of certification and assessment services, and for providers of project tools and infrastructure, and it would accelerate the careers of qualified project professions who are capable of operating at a high maturity score on the cybersecurity perspective.

About the Authors

Jay Payette is a graduate student in the Masters of Design program at Carleton University in Ottawa, Canada, and is the Managing Principal of Payette Consulting. Jay founded Payette Consulting in 2011 to help clients balance the consistent results of repeatable business processes and analytic decision making, with the fuzzy world of creativity. His research has focused on applying design-thinking principles to business model generation, strategy, and project delivery. Prior to founding Payette Consulting, Jay worked for the Canadian consulting practice of Accenture and as an independent IT Project Manager.

Esther Anegbe is a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She also holds a Bachelor's degree in Computer Engineering from Ladoke Akintola University of Technology in Nigeria. She worked as a Technology Analyst with a leading Investment Management Firm in Lagos, Nigeria (Sankore Global Investments), where she formed part of the technology team that developed, deployed, and provided support for the financial software projects that expanded the market reach of the firm’s stock brokerage and wealth management subsidiaries. She is currently working on a startup (Tech Wits) to provide enterprise solutions and services to startups in their accelerators and incubators.

Erika Caceres is a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She holds a Bachelor's degree in Technology Information Management from The University of Yucatan, Mexico. She previous worked as an innovation consultant at I+D+i Hub, a leading technology transfer office in Merida, Mexico, where she formed part of the management team to produce innovation projects that were submitted for funding to the government to help accelerate the economy in the south of Mexico. She is currently working on Volunteer Safe, an online startup that pre-screens and licenses volunteers and connects them to volunteer opportunities aligned to their profile.

Steven Muegge is an Assistant Professor at the Sprott School of Business at Carleton University in Ottawa, Canada, where he teaches and leads a research program within Carleton’s Technology Innovation Management (TIM) program. His research, teaching, and community service interests include technology entrepreneurship and commercialization, non-traditional settings for innovation and entrepreneurship (business ecosystems, communities, platforms, and interconnected systems that combine these elements), and business models of technology entrepreneurs (especially in non-traditional settings).

References

Bailey, T., Del Miglio, A., & Richter, W. 2014. The Rising Strategic Risks of Cyberattacks. *McKinsey Quarterly*, May: 17–22. http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks

Brookes, N., & Clark, R. 2009. Using Maturity Models to Improve Project Management Practice. In *Proceedings from the POMS 20th Annual Conference*, Orlando, FL, May 1–4.

Caralli, R. A., Allen, J. H., & White, D. W. 2010. *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience* (CERT-RMM Version 1.1). Boston, MA: Addison-Wesley Professional.

Carbone, P. 2007. Competitive Open Source. *Open Source Business Resource*, July: 4–6. http://timreview.ca/article/93

Ellison, R. J., Goodenough, J. B., Weinstock, C. B., & Woody, C. 2010. *Evaluating and Mitigating Software Supply Chain Security Risks.* No. CMU/SEI-2010-TN-016. Software Engineering Institute, Carnegie-Mellon University: Pittsburgh, PA.

Golden, B. 2008. Making Open Source Ready for the Enterprise: The Open Source Maturity Model. *Open Source Business Resource*, May: 4–9. http://timreview.ca/article/145

Hughes, J., & Cybenko, G. 2013. Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. *Technology Innovation Management Review*, 3(8): 15–24. http://timreview.ca/article/712

Humphrey, W. S. 1988. Characterizing the Software Process: A Maturity Framework. *IEEE Software*, 5(2): 73–79. http://dx.doi.org/10.1109/52.2014

Kerzner, H. 2013. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling* (11th ed.). Hoboken, NJ: John Wiley & Sons.

McGraw, G. 2006. *Software Security: Building Security In.* Upper Saddle River, NJ: Addison-Wesley.

Merkow, M. S., & Raghavan, L. 2012. *Secure and Resilient Software: Requirements, Test Cases, and Testing Methods.* Boca Raton, FL: CRC Press.

Milosevic, D., & Patanakul, P. 2005. Standardized Project Management May Increase Development Projects Success. *International Journal of Project Management,* 23(3): 181–192. http://dx.doi.org/10.1016/j.ijproman.2004.11.002

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

NIST. 2014. *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.0. Gaithersburg, MD: National Institute of Standards and Technology. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Office of Government Commerce. 2006. *Portfolio, Programme and Project Management Maturity Model (P3M3).* London: The Stationary Office.

Office of Government Commerce. 2009. *Managing Successful Projects with PRINCE2* (2009 ed.). London: The Stationary Office.

Pfleeger, C. P., Pfleeger, S. L., & Margulies. 2015. *Security in Computing* (5th ed.). Upper Saddle River, NJ: Prentice-Hall.

Phillips, J. 2010. *IT Project Management: On Track From Start to Finish* (3rd ed.). New York: McGraw-Hill.

PMI. 2013a. *A Guide to the Project Management Body of Knowledge* (PMBOK Guide) (5th ed.). Newton Square, PA: The Project Management Institute.

PMI. 2013b. *Organizational Project Management Maturity Model* (OPM3) (3rd ed.). Newton Square, PA: The Project Management Institute.

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

Sowden, R., Hinley, D., & Clark, S. 2013. *Portfolio, Programme, and Project Management Maturity Model (P3M3): Introduction and Guide to P3M3,* Version 2.1. London: AXELOS Limited. https://www.axelos.com/Corporate/media/Files/P3M3%20Model/P3M3_Introduction_and_Guide.pdf

The President. 2013. *The President of the United States: Executive Order 13636—Improving Critical Infrastructure Cybersecurity.* Federal Register/Presidential Documents, 78(33): February 19, 2013. Washington, DC: U.S. National Archives and Records Administration. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

U.S. Department of Energy. 2014. *Cybersecurity Capability Maturity Model* (C2M2 v1.1). Washington, DC: U.S. Department of Energy. http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014

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

Young, R., Young, M., & Zapata, J.R. 2011. *A Critical Assessment of P3M3 in Australian Federal Government Agencies.* Canberra, Australia: ANZSOG Institute for Governance, University of Canberra. http://www.governanceinstitute.edu.au/magma/media/upload/media/529_P3M3-Anzsig-Insight.pdf

Citation: Payette, J., Anegbe, E., Caceres, E., & Muegge, S. 2015. Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects. *Technology Innovation Management Review,* 5(6): 26–34. http://timreview.ca/article/904

Keywords: project management, critical infrastructures, cybersecurity, capability maturity models, CERT RMM, NIST, C2M2, P3M3, PjM3