Adoption of Cybersecurity Capability Maturity Models in Municipal Governments

Walter Miron

A thesis submitted to the Faculty of Graduate Studies in partial fulfillment

of the requirements for the degree of

Master of Applied Science

in

Technology Innovation Management

Faculty of Systems and Computer Engineering

Carleton University

Ottawa, Ontario

Abstract

Cyberattacks are increasing in diversity and volume placing information and communications technology (ICT) as well as physical assets at risk. Municipal governments operating as the provider of an interdependent network of e-government services, Information and Communications Technology, and Critical Infrastructure (CI) have a requirement to quickly, easily, and inexpensively secure their ICT systems and physical assets.

In addition to other sources, this study sampled data from Canadian municipal government CIO's using expert interviews followed by a web-based survey in the winter of 2015 to help inform both the development of a Cybersecurity Capability Maturity Model for Canadian municipalities and to provide recommendations pertaining to the adoption of such a model.

The study confirmed the low level of recognition by Canadian municipalities regarding Cybersecurity Capability Maturity Models (CCMM) and identified a need to improve their observability in this sector in order to foster adoption. Simplicity of the CCMM and its Trialability in municipal CI networks emerged as key factors influencing its adoption and these factors are considered in the development of the CCMM. Compatibility of the CCMM did not emerge as a factor in adoption as they are new to municipal CI protection. A model combining controls from ISO 27000 and maturity scoring based on SEI-CMMI maturity levels is developed to simplify cybersecurity readiness maturity assessment, and a model for diffusing the CCMM in Canadian municipalities is provided.

Table 1: List of Abbreviations

AES	Advanced Encryption Standard
ANOVA	Analysis of Variance
CAO	Chief Administrative Officer
CEO	Chief Executive Officer
CERT	Computer emergency response team
CI	Critical Infrastructure
CIO	Chief Information Officer
CCMM	Cybersecurity Capability Maturity Model
CMM	Capability Maturity Model
CSO	Chief Security Officer
CTO	Chief Technology Officer
DOI	Diffusion of Innovation
ICT	Information and Communications Technology
IS	Information Security
ISMS	Information Security Management System
ISO/IEC	International Standards Organization / International Electotechnical Commission
MISA	Municipal Information Systems Association of Canada
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard
RFP	Request for Proposal
RMM	Risk and Resilience Management
SEI	Software Engineering Institute
UTF	Universal Character Set Transformation Format

Table of contents

List of figures

List of tables

Acknowledgements

First, I would like to thank my supervisor Dr. Tony Bailetti for the support and mentorship that he has given me throughout my journey at Carleton University. You have gone far beyond the role of professor and I sincerely appreciate your advice on academics, research, work, and family.

Second, I would like to thank my manager, mentor, and friend Ibrahim Gedeon. Without Ibrahim's support the completion of this degree would have not been possible. Your example, advice, and high-standards have inspired me to continually improve my work and academic careers.

Third, I would like to acknowledge Professors Muegge, Weiss, and Westerlund for their feedback and insight through my thesis development, Barton McKinley, Dan Craigen, and Ali Tizghadam for their feedback and advice through the study, and Ms. Emily Byron for her timely answers to my many questions.

Finally, I would like to thank my wife Jennifer, daughter Emma, and son Ethan for their patience, understanding, and seemingly endless support of my studies, without which I would not have been able to undertake this exciting and rewarding challenge.

1 Introduction

The rapid increase in frequency and diversity of cyberattacks has placed technology managers under pressure to secure the information and physical assets that they provide stewardship over. As providers of critical infrastructure, municipal governments face an increased duty to protect the assets of their constituents, the compromise of which has potential to risk security of data, financial impact, damage, and injury or loss of life. Protecting the Information and Communications Technology (ICT) and physical assets, which control this critical infrastructure, is therefore a paramount concern for the operators of critical infrastructure in Canada.

Municipal government CIO's require a method to consistently assess the readiness of their critical information and communications technology infrastructure to withstand cyberattacks, to identify and remediate gaps in their capabilities, and to report on their status in order to meet industry and regulatory compliance requirements. As operators of multiple interdependent networks of critical infrastructure municipal government CIO's face a unique challenge in addressing the complexity that this interdependence poses to the cybersecurity of their assets.

The scholarly and practitioner management literature has reviewed critical infrastructure (CI), information security (IS), information and communications technology (ICT) security, and capability maturity models (CMM) individually and in various combinations. Much of this literature has taken a general view of issues in these domains, focusing on broader policy concerns. There is a body of practitioner literature in these domains that provides a narrow focus on issues in specific subdomains such as water treatment and delivery or energy delivery. Capability Maturity Models for specific domains such as SSE-CMM, ES-C2M2, ONG-C2M2, NICE-CMM, CERT-RMM have been developed (Table 4). However, none of these examples

address the interdependency of municipal critical infrastructure and information and communications technology. Further, these models do not prescribe specific controls for the cybersecurity readiness of information and communications technology used to control critical infrastructure assets. ISO/IEC 27000 is an Information Security Management System (ISMS) protocol that specifies controls for the cybersecurity of information technology, however it is not specific to interdependent systems, nor does it address detailed progressions towards cybersecurity readiness goals as in a CMM. It is a pass or fail assessment model conducted at a specific point in time.

A search on Google Scholar for the words "cybersecurity CMM municipal" anywhere in the article with no restrictions on publication date returned 37 matches. Of these matches only one unpublished scholarly article and 5 reputable conference presentations were found. The remainder were comprised of 9 books, 4 practitioner articles from Internet journals, and 18 blog or web articles. In contrast, omitting CMM from the search criteria and searching for "cybersecurity municipal" on Google Scholar returns 2330 matches showing that cybersecurity of municipal governments is of interest to the research and practitioner communities, and that there is an opportunity to study the impact of cybersecurity CMMs in this domain.

Thus there is a need for a Capability Maturity Model aimed at the consistent and progressive implementation of controls for the security of information and communications technology used in the operation of municipal critical infrastructure assets.

The aim of this research is to develop such a Cybersecurity Capability Maturity Model (CCMM) for Canadian municipalities and to provide recommendations on the adoption of such a model. These are particularly challenging tasks given the low level of recognition by Canadian municipalities regarding Cybersecurity Capability Maturity Models.

Through our sampling of data from Canadian municipal government CIO's using expert interviews followed by a web-based survey in the winter of 2015, we incrementally developed both a Cybersecurity Capability Maturity Model for Canadian municipalities and a model for its diffusion through Canadian municipalities.

In the researcher's opinion, the CCMM will promote the regular self-assessment of cybersecurity readiness and provide a means to report progress towards cybersecurity goals. This will be of significance to municipal CIOs who are tasked with easily, quickly, and cost-effectively securing their critical infrastructure, to service and product providers who wish to bring their products to market and to researchers through opportunities to further the study.

1.1 Objective

The objective of this study is to investigate how, why, and at what rate a Cybersecurity Capability Maturity Model (CCMM) will spread through Canadian municipalities, to develop such a CCMM for Canadian municipalities, and to develop a model for the adoption of such a CCMM.

To inform the adoption model the five factors of the diffusion of innovation theory; Relative Advantage, Compatibility, Complexity, Trialability, and Observability (Rogers, 2003) are of particular pertinence. Interviews of experts in cybersecurity, critical infrastructure protection, and municipal CIO's followed by a short web-based survey were used to comprehend these five factors shown in table 2. Rogers diffusion of innovation was selected as a framework to base this research study on as it is well known with a large number of citations and widely understood concepts such as the five factors and five stages of innovation. The study was constrained to

Canadian municipalities as operators of multiple, interconnected cyber-interdependent critical infrastructures due to the criticality of securing these assets. Focus was placed on adding capability maturity modelling to readiness assessments in order to promote a proactive approach to cybersecurity of the assets and to encourage incremental improvements in CI protection. Specific cybersecurity elements such as network firewalls, virus checkers, denial of service scrubbers and the like were excluded from the study as they are covered esoterically in the ISO controls, and are considered to be point solutions in the overall process.

Table 2: CCMM questions mapped to Rogers five factors

Relative advantage:	Are CCMMs better than existing methods to assess readiness
Compatibility:	Will CCMMs require large changes to CIO's routine?
Complexity or simplicity:	Are CCMMs easier for CIOs to use?
Trialability:	Can the CIO easily trial the use of CCMMs in their environment.
Observability:	Are CCMMs known and positively perceived by CIOs

Rogers DoI five factors (Rogers, 2003)

The results from this research will be used to incrementally develop a cybersecurity capability maturity model comprised of ISO/IEC27000 controls and SEI-CMMI maturity scoring and to develop a model for its diffusion in Canadian municipal governments.

1.2 Deliverables

This study has two deliverables:

- A Cybersecurity Capability Maturity Model (CCMM) for Canadian municipalities
- A model for adoption of the CCMM by Canadian municipalities

1.3 Relevance

This research problem is relevant to Municipal government CIOs, their constituents, services and product providers, and researchers by extending their knowledge of the domain, understanding the factors impacting model adoption, and leveraging these factors in the development of a business model for the diffusion of the CCMM in the industry.

Municipal government CIOs will find this study interesting as it will address their need for a method to easily, quickly, and cost-effectively secure their critical infrastructure. Validating and improving cybersecurity capability maturity models for their use will simplify the task of improving and reporting on their cybersecurity readiness.

Constituents will benefit from the results of this study through improved security of their data and the critical infrastructure that they rely on for normal societal function, as well as through efficient use of publicly owned resources.

Service and product providers wishing to bring their products to market will find this study interesting by understanding the key issues facing municipal CIOs, use of the CCMM as a guide for cybersecurity, and leveraging this understanding to enhance their resulting business models.

Researchers will find relevance in this study through its contribution to the scholarly literature on the use of capability maturity models in critical infrastructure cybersecurity protection, and thorough opportunities to further the study by refining the research question, conducting a longitudinal study in this domain, and refinements to the CCMM.

1.4 Value of the deliverables

Based on our understanding of other Capability Maturity Models and adoption, we expect the deliverables of this study to provide value in four ways.

- De-risk the municipal technology managers role in securing critical infrastructure through the introduction of a consistent protocol for implementation and assessment of cybersecurity readiness
- The CCMM reduces the time and cost to municipalities of cybersecurity compliance and reporting
- Increased frequency of cybersecurity readiness assessments
- Improved cybersecurity and reporting of municipal critical infrastructure

Canada is comprised of over 4000 municipalities ranging in population size from a few to millions of constituents. Unsystematic implementation of cybersecurity protections increases the risk of cyberattack (Chapin and Akridge, 2005). The adoption of a CCMM for Canadian municipalities will reduce the risks faced by municipal technology managers in securing critical infrastructure by providing a framework for the consistent application of security protocols and assessment of cybersecurity readiness. Further, a viable ecosystem of product and service providers will facilitate timely and cost-effective adoption of the CCMM.

A systematic and consistent implementation of CCMMs will lead to improved cybersecurity for critical municipal ICT infrastructure, and allow municipal CIOs a common approach to reporting of cybersecurity readiness for regulatory and industry purposes.

1.5 Overview of method and expected results

This study uses a seven-step method to conduct the research:

1. The management and practitioner literature was reviewed to develop an initial version of the CCMM and adoption model.
2. These initial models were reviewed with experts and refined by incorporating their feedback into version two of the documents.
3. Based on these models, a questionnaire was developed for use in the cross-sectional study.
4. Once approved by the university research ethics board, the survey was validated with expert advice.
5. Learning's from this exercise were incorporated into a refined version of the survey instrument.
6. A simple random sample of Canadian municipalities was selected at which time the large sample survey was conducted.
7. The results from the data analysis were applied to improve the CCMM and adoption model.

1.6 Organization of the thesis

This thesis is organized as seven chapters, each structured into sections and subsections. Chapter 2, "Literature review," reviews the scholarly literature. It is organized into three streams; Critical Infrastructure, Capability Maturity Models, and Diffusion of Innovation theory. Chapter 2 concludes with a synthesis of the literature. Chapter 3, "Research design and method," describes the method used in the study and is divided into 5 sections; A review of the method, research design, data acquisition, data analysis, and a summary. Chapter 4 presents the research results. Chapters 5 and 6 are a discussion of the results and conclusions, respectively. Chapter 7 contains

references to the literature. Appendices will include the CCMM, adoption model, survey response data, and survey and interview instrument documents.

2 Literature review

The literature review is organized as 3 streams and summarizes the constructs and insights salient to this thesis. The first stream covers critical infrastructures and their interdependencies. The second stream reviews capability maturity models and their relation to cybersecurity, and the third stream reviews diffusion of innovation theory. The chapter concludes with a summary and synthesis of the lessons salient to this research.

2.1 Critical infrastructure

The first stream is Critical Infrastructure (CI). CI is defined as "any element, system or part thereof, situated in a state that is considered essential for the maintenance of vital societal functions, health, physical integrity and security, social and economic welfare." (Yusta et al., 2011; Murray & Grubesic, 2012; Singh et al., 2014). Thirteen sectors are defined as critical infrastructures; food supply, banking and finance, telecommunications, defense, emergency services, energy, healthcare, information technology, national monuments, shipping, transportation, and water distribution (Singh et al., 2014). Of these thirteen sectors water and energy management, and communications systems are thought of as lifeline utility systems (Poljansek et al., 2012). Public Safety Canada narrows this list to ten categories; Health, Food, Finance, Water, Information and Communication Technology, Safety, Energy and utilities, Manufacturing, Government, and Transportation (Canada, 2014).

"More than an abstract theoretical concept," (Rinaldi et al., 2001), modern critical infrastructures are complex systems comprised of collections of interconnected systems (Merrabti et al., 2011) and have dependencies on one another (Singh et al., 2014). To illustrate the dependency between

the CI sectors, the interpreted structural modelling (ISM) diagram (figure 1) depicts the relationship between the critical infrastructure sectors. The electrical sector is of the highest depth, having the most "driving power" of the sectors, meaning that all sectors are directly or indirectly related to it. The information technology and communications sectors are one level of driving power lower, being driven by the electrical sector creating a dependency on it. They in turn drive other CI elements and are directly or indirectly related to all other sectors, showing their importance in terms of critical infrastructure hierarchy.

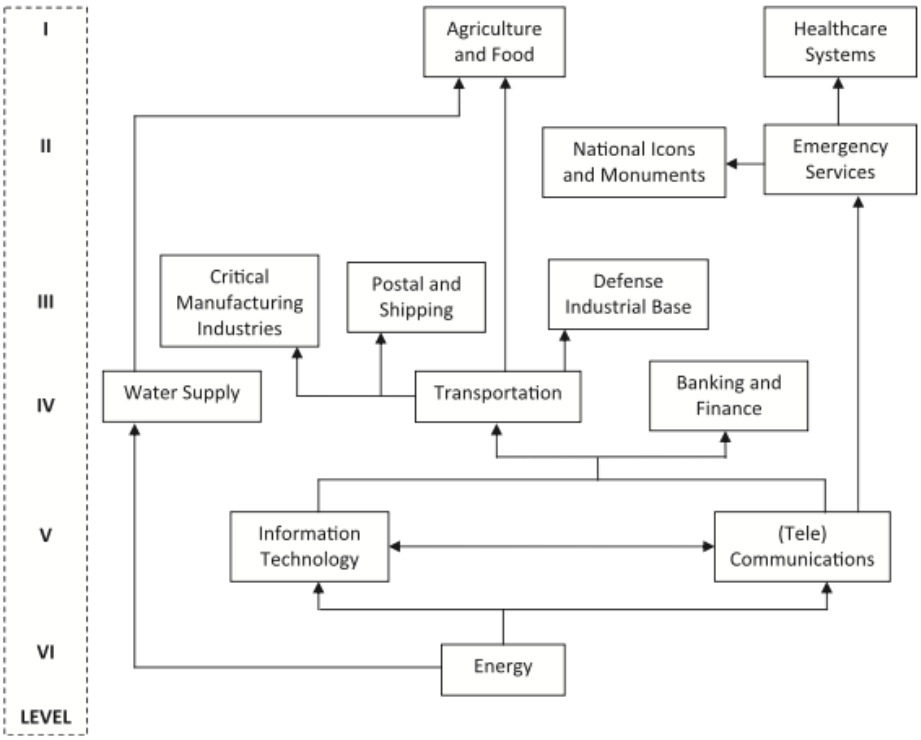

Figure 1: Critical Infrastructure Interdependencies (Singh et al., 2014)

Interdependence of infrastructures can lead to cascading failures where a failure in one system propagates to a connected system, (Vespignani, 2010). The interdependence of connected networks of infrastructure result in their fragility compared to isolated systems, causing them to fail rapidly and abruptly when compared to isolated networks (Buldyrev et al., 2010; Vespignani, 2010). CI must be secured at both the macro and sub-element levels (Merrabti et al., 2011) so

these interdependencies must be considered in modern CI network design (Buldyrev et al., 2010). Information and communications technology (ICT) is used for the control of modern critical infrastructures, presenting a cyber-interdependency (Rahman et al., 2011). And, as the attack surface increases due to ever increasing connectivity (Dupont, 2013; Mellado et al., 2010) and suppliers bring products to market with inadequate security (Dupont, 2013), a need has arisen to consider vulnerabilities in this domain in CI protection (Merrabti et al., 2011). When considering that modern critical infrastructure has both dependencies between the sectors and utilizes elements for control that have cyber-interdependencies, this complexity presents resiliency and security design challenges (Xiao-Juan & Li-Zhen, 2010; Rahman et al., 2011) as well as influencing operational factors (Rinaldi et al., 2001).

Given the importance of CI and the difficulty of securing this unique class of interdependency (Rahman et al., 2011; Miron & Muita, 2014), standards bodies and federal agencies have defined best practices for its security with compliance models developing in both regulatory regimens (European Union) and public – private cooperation (US) (Yusta et al., 2011). Most recently, New York State has introduced legislation to ensure the security of some critical infrastructure assets and the status reporting of readiness (N.Y. State Senate, 2015). Table 3 shows examples of cybersecurity regulations and frameworks in western countries.

Table 3: Examples of cybersecurity regulations and frameworks (Miron & Muita, 2014)

Region	Regulation	Model
European Union	European Programme for Critical Infrastructure Protection (EPCIP)	Regulation
Canada	National Strategy for Critical Infrastructure (NSCI)	Cooperative Framework
United Kingdom	Centre for the Protection of National Infrastructure (CPNI)	Cooperative Framework
United States	National Infrastructure and Protection	Cooperative Framework

Plan (NIPP 2013)

These frameworks recognize the geographic interdependency of CI and offer high-level guidance on securing it. Miron and Muita explain.

> *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* (Miron & Muita, 2014).

The literature on critical infrastructure informs that the sectors of critical infrastructure have dependencies between them that cause one sector to act upon another with the potential to incur cascading effects when failures arise. These CI rely upon information and communications technology for their operation, introducing a further relationship termed cyber-interdependency. Cyber-interdependencies introduce complexity in adequately securing these resources, and these complexities form a scenario that is not resolved in current cybersecurity frameworks, regulations, and controls.

2.2 Capability Maturity Models

The second stream in the literature review is Capability Maturity Models (CMM). CMMs are a tool originating in the software engineering discipline to provide a simple method for measuring a progression of process capabilities through a sequence of levels toward a target state (Becker et al., 2009; Lahrmaan et al., 2011; Wendler, 2012). To do this CMM's provide guidance on measuring progress towards specific target states as well as criteria for advancing through the maturity levels (Wendler, 2010). CMMI is one example of a CMM. It uses 6 levels for measuring

capability maturity in its design; 0 – non-existent, 1 – initiating, 2 – Managed, 3 – Defined, 4 – Quantitatively Managed, and 5 – Optimizing (Debreceny, 2006). The systemic engineered approach of CMMI allows the prediction of control failures using the maturity level (Debreceny, 2006). The output of CMM's provide pragmatic advice for decision makers on the advancement of their capabilities (Lahrmaan et al, 2011). In order to remain relevant, CMM's must be developed and evaluated iteratively, and should provide methods for self-assessment of capabilities by practitioners (Becker et al., 2009, Lahrmann et al., 2011). Acceptance of a CMM is dependent on its utility and validity (Lahrmann et al., 2011). Many current maturity models for specific domains have been based on CMM/CMMI from the software engineering institute and ISO/IEC 15504 SPICE (Software Process Improvement and Capability dEtermination) (Von Wagenheim, 2010). CMMs have been developed for cybersecurity in specific domains such as energy, water supply, and oil and gas distribution.

Applied to cybersecurity, CMMs are an important tool as unsystematic implementations of cybersecurity protections increase the risk to vulnerabilities (Chapin & Akridge, 2012). Further, while regulatory regimens may not dictate compliance, financial control compliance requirements like the Sarbanes Oxley act require systemic consistent methods for assessing and reporting internal control maturity (Debreceny, 2006). Cybersecurity CMMs can benefit from the experience of CMM's from the systems engineering discipline in their evolution (Siponen, 2002). They must be ISMS related and not related solely to computer security (Siponen, 2002). Table 4 summarizes available capability maturity models for resiliency and security.

Table 4: Cybersecurity capability maturity models for critical infrastructure (Miron & Muita, 2014)

Model	Publisher	Purpose
C2M2	US Dept. of Energy	Assessment of cybersecurity capabilities for any organization comprised of a maturity model and evaluation tool

ES-C2M2	US Dept. of Energy	C2M2 tailored to energy subsector
ONG-C2M2	US Dept. of Energy	C2M2 tailored to the oil and natural gas subsector
NICE-CMM	US Dept. of Homeland Security	Defines three areas: process and analytics, integrated governance, skilled practitioners and technology for workforce development
CERT-RMM	CERT/SEI	Defines organizational practices for operational resilience, security, and business continuity
ISO/IEC 15408	ISO	Criteria for computer security certification
ISO/IEC 27001	ISO	Information Security Management System (ISMS) specification
ISO/IEC 21827 SSE-CMM	ISO	Evaluation of software security engineering processes
NIST Cybersecurity Framework	NIST	Framework for improving federal critical infrastructure through a set of activities designed to develop individual profiles for operators

These maturity models provide operators guidance on the development of cybersecurity readiness plans at a high-level (Miron & Muita, 2014). Of these models, only the ISO standards provide prescriptive guidance for cybersecurity readiness, though they are complicated and costly to deploy (Miron & Muita, 2014).

2.3 Diffusion of Innovation

The final stream is Diffusion of Innovation.

Rogers (2003) tells us that there are five factors that affect the Diffusion of Innovation or adoption of innovation. Relative advantage compares the innovation to the current product or method. Compatibility considers the introduction of the innovation on current activities or processes. Complexity or simplicity relates to the ease of use of the innovation and impacts its adoption. Trialability considers the ease with which an innovation can be tested. Observability is

the level of exposure that a technology has to the market. Peres et al. (2010) adds that social influences are another factor impacting the adoption of innovation. Social signals; the act of adopters following consumption behaviours of others, and network externalities or effects; factors promoting or detracting adoption such as hardware and software compatibility, are examples of social influences.

Groups of individuals with similar attributes tend to cluster together. Rogers (1983) termed this homophily. Homophilous groups share tight bonds and this trust leads them to share ideas and adopt ideas together (Adams et al., 2014; Rostila, 2010). Homophilous groups may not be exposed to innovation early however because of these tight bonds (Adams et al., 2014; Rogers & Bhowmik, 1970). Therefore in order to adopt an innovation early a group that has a mix of homophily to allow trust and heterophily to introduce the innovation is required to foster adoption of innovation as it produces an environment where differing perspectives can be considered (Rogers & Bhowmik, 1970).

Adoption decisions in organizations are influenced by both individual and organizational motivations, norms, and procedures (Greenhalgh et al., 2004). Decision-making in organizations can be categorized into two types Collective Innovation Decision; a decision made collectively by group members, and Authority Innovation Decision; a decision made by power brokers and authority figures for the entire organization. In both cases, "*champions*" in the organization are required to promote the innovation. Organizations require an impetus, or tension for change, in order to adopt an innovation (Rogers, 1983). Industry, community, or economic pressures influence organizational decision making (Gustafson et al., 2003). A tension for change in the instance of cybersecurity could be a regulatory imperative such as the recent New York State legislation introduced to ensure that critical infrastructure is secured and that agencies report on their status (N.Y. State Senate, 2015), or the potential consequences of legal actions resulting

from exploits where controls were available and were not applied by operators (Gregory, 2014; Nili, 2014), or compliance with financial regulation such as the Sarbanes Oxley act (Debreceny, 2006).

Diffusion of innovation also considers the consequences associated with adoption or non-adoption of an innovation. Rogers (1983) defines types of consequences as Desirable vs. undesirable, Direct vs. indirect, and anticipated vs. unanticipated. Wejnert (2002) defines consequences in two categories; Public, consequences by an actor on others, and Private, consequences on the actor. In these cases, decision makers consider the consequences of acting or not acting in their adoption of an innovation.

2.5 Lessons learned from the literature

In summary, the salient lessons for this literature review include the following.

Modern critical infrastructure elements are highly dependent on the information and communications technology used for its operation and control. As such, it is vulnerable to information security exploits. The CI elements are dependent on one another, and the interdependence of these connected CI elements constitutes a complex system that is difficult to secure. Failures in one system pose a risk to other connected systems. Therefore, the consistent application of information security controls is imperative to the safe and secure operation of modern critical infrastructure systems.

Capability maturity models, originally designed in the software engineering domain to improve process capability over a continuum of time, are germane to the cybersecurity domain. They can be used to consistently apply, measure, and improve information security controls in order to

mitigate threats to critical infrastructure systems. While current cybersecurity capability maturity models such as SSE-CMM, C2M2, ES-C2M2, ONG-C2M2, NICE-CMM, CERT-RMM exist, they are complicated, require specialized skillsets to implement and manage, lack maturity measurements, and none specifically address the interdependency of municipal CI and ICT. There is an opportunity to improve cybersecurity by developing a CCMM for municipal critical ICT infrastructure, and to improve adoption of CCMMs

Diffusion of innovation theory, particularly the five factors impacting adoption of innovation, is applicable to the adoption of CCMMs in municipal government critical infrastructure protection. Organizations have different approaches to and considerations in their decision making, with different tensions for change and motivations to be contemplated. Group decisions require a mix of members with strong social ties building trust, and external influences with a knowledge of an innovation in order to promote the adoption of an innovation in their organizations.

This chapter has reviewed the scholarly literature on Critical Infrastructure, Capability Maturity Models and Cybersecurity Capability Maturity Models, and the Diffusion of Innovation. The next chapter presents the research design and method.

3 Research design and method

This chapter presents the research design and detailed methods to answer the research question posed in chapter 1; how, why, and at what rate will a CCMM diffuse in Canadian municipalities. The chapter is structured in five sections; A review of the method, the research design, data acquisition, data analysis, and a summary.

3.1 Research Method

This section discusses the process used to conduct the study and the outcomes of the stages of the process.

The study includes an iterative approach to building a CCMM for Canadian municipalities and a model to diffuse the CCMM to Canadian municipal government critical infrastructure cybersecurity. An initial version was drafted using the management literature, and validated by an expert panel familiar with cybersecurity, critical infrastructure protection, and municipal ICT cybersecurity practices. Feedback from the panel was then used to improve the initial models.

A survey instrument was then designed to capture demographics for cluster analysis, knowledge of ISO/IEC 27000 and SEI-CMMI, use of these two methods (or other CMMs) for cybersecurity, and factors that will impact adoption of the model. Once approved for use by the university research ethics board a survey research expert validated it. Using the validated questionnaire, a large-scale cross-sectional survey was used to obtain a sample of 42 CIO's, practitioners, and decision makers in Canadian municipalities.

Data was analysed using one-way analysis of variation tests (ANOVA) to determine the

improvements to the CCMMs and adoption model, which resulted in a final version of the models for delivery.

Table 5 summarizes the activities and outcomes of the research method used in this study.

Table 5: Research method summary

Step	Dominant activity	Outcome
1	Review the critical infrastructure, CCMM, diffusion of innovation, and e-government literature streams and develop the first version of the models	Version 1 of: • CCMM • Adoption model for CCMM
2	Develop a refined model by interviewing and incorporating the feedback from 3 experts	Version 2 of: • CCMM • Adoption model for CCMM
3	Design questionnaire and gain approval to use it	Approved version 1 of questionnaire for CIOs of municipalities
4	Validate questionnaire with survey research expert	Version 2 of questionnaire for CIOs of municipalities
5	Divide Canadian municipalities into clusters and select a simple random sample of each group	Sample
6	Conduct survey	Questionnaires completed by CIO's of municipalities
7	Assess responses to survey	• Determine improvements to CCMMs • Determine key opportunities for improving adoption of the CCMM by Canadian municipalities
8	Provide models	Version 3 of: • CCMM • Adoption model for CCMM

3.2 Research Design

The research design section describes the unit of analysis, sample selection, and sampling process.

The unit of analysis for this study is the completed questionnaire responses from the CIOs, practitioners, and decision makers in Canadian municipalities.

A cross-sectional web-based survey was used to draw the sample from January to March 2015. The sample of 42 respondents was drawn from a population of CIOs, practitioners, and decision makers in 4748 Canadian municipal governments.

The population was clustered into three groups categorized by municipal population; small, medium, and large. A larger sample provides normal distributions so a minimum sample size of 71 respondents was sought. Municipal residential population taken from 2011 federal census data obtained from Statistics Canada shows that there are 4748 municipalities in Canada, which provides an acceptable population. However, as there are only three cities in Canada with a population over 1 million residents, and 11 cities with over 500,000 residents, the large municipality cluster was set at municipalities with over 500,000 residents. This provides a small sample for this particular cluster so the entire population was targeted. The remaining clusters are of adequate size.

Table 6 depicts the cluster structure

Table 6: Survey Sample structure

Cluster	Municipality Size	Random Sample Size			Expected Response rate		Targeted sample size
	Residents	Population	%	#	%	#	#
Small	< 10k	4350	20	870	10	87	30
Medium	10K – 500K	387	78	301	10	30	30
Large	> 500K	11	100 Targeted	11	100 Targeted	11	11

3.3 Data Acquisition

The data acquisition section describes the data that was used to produce the deliverables, how it was obtained, and where the sample was drawn.

Variables reflecting the respondents' demographics, knowledge of capability maturity models and cybersecurity protocols, factors impacting adoption of a CMM, and other information the respondent deemed important for the study were assigned to the data collected. Table 7 depicts the mapping of the variables to the research question and question type as per (Creswell,

2014:162). The variables are analysed in Stata 13 using ANOVA testing.

Table 7: Table of variables

Theory	Variable	Answers?
Demographics	CIS	What does the respondent manage?
Demographics	EXP	Does tenure impact perspective?
Demographics	POP	Do different sized municipalities have different challenges or capabilities
Demographics	ROL	Do different roles have different perspectives?
Model	CMM1	Do different sized municipalities have different challenges or capabilities
Model	CMM2	Do different roles have different perspectives?
Model	CMM3	CMM's used
Model	CMM4	Knowledge of ISO/IEC 27000
Model	CMM5	Knowledge of SEI-CMMI
Comments	Comments	Other feedback
Compatibility	Comp_1	Determine if compatibiity of the CMM impacts adoption
Compatibility	Comp_3	Assess the impact of compatibility on adoption time of CMM
Observability	obsv_1	Observability that interdependence of CI impacts readiness
Observability	obsv_2	Observability that interdependence poses difficulty in securing the resources
Observability	obsv_3	Perception of regulatory environment
Observability	obsv_4	Observability of industry adoption
Observability	obsv_5	Observabilty of cybersecurity
Relative Advantage	RA_1	Assess current state in order to determine RA of CMM
Relative Advantage	RA_2	Assess perception of efficacy of the CMM
Relative Advantage	RA_3	Set baseline for RA assessment
Relative Advantage	RA_4	Assess the impact on adoption time of CMM use
Complexity or Simplicity	Simp_2	Whether the perception is important
Complexity or Simplicity	Simp_3	Assess the impact on adoption time of ease of use of the CMM
Trialability	trial_1	Trialability of a CMM
Trialability	trial_2	Determine what manifestations of a CMM would lead to a successful trial
Trialability	trial_3	What is the anticipated reduction in implementation time by trialing first?

Data was acquired during the two phases of the study; interviews with IT Security Experts, and a short online survey designed to measure the impact of CMMs on cybersecurity readiness. Prior to conducting the survey the method and survey instruments were reviewed and approved by the Carleton University Research Ethics Board. All data collected during the study is anonymized and the dataset is stored using AES256 encryption on secure servers located in Canada with access restricted to the researchers. Data was exported to an excel file using UTF-16 comma separated formatting and to Stata 13 for further analysis.

In designing the survey instruments several biases were considered in order to minimize the effect of non-sampling errors on the total survey error.

To minimize researcher or survey bias preliminary research was conducted with literature reviews and expert interviews (Foddy, 1993:6). The sample was drawn from the population of Canadian municipalities using a random sample invited through the Municipal Information Systems Association of Canada (Creswell, 2014:158; Babbie, 2007), and through stratification of the respondents based on municipal population (Creswell, 2014:158; Fowler, 2009) in order to minimize population definition and sampling frame errors.

As municipal cybersecurity is anticipated to be a sensitive topic with respondents, efforts were taken to minimize respondent or social desirability bias as well as non-response bias. Survey participants were offered opt out choices using" I don't know" as a response choice and allowing respondents to bypass a question rather than answer it falsely or in ignorance (Foddy, 1993:8). Links to background information and definitions were provided to set context for respondents (Foddy, 1993:20). Legitimacy of the study was improved by the sponsorship of Carleton University, Public Works and Government Services Canada, and the Municipal Information Systems Association of Canada. Additionally, confidentiality and security of the respondent's data was assured.

To minimize response bias questions were ordered from general to specific so as not to influence responses (Foddy, 1993:7, 61) and question wording was clarified to remove abstract words and avoid pre-positioning answers in order to reduce interpretation by the respondents (Foddy, 1993: 41,44). Questions were crafted minimizing the number of responses and with the use of scales to minimize respondents reading long lists of answers (Foddy, 1993:157). Finally, participants were allowed to navigate the survey giving them visibility to all answer options (Foddy, 1993: 169).

In the first phase of the study, interviews were conducted with an expert panel familiar with cybersecurity, critical infrastructure protection, and municipal ICT cybersecurity practices. The interviewees were asked open and closed questions designed to solicit input on the observability of critical infrastructure dependency, cyber-interdependency, best practices within the municipal critical infrastructure ICT community, and perception of ISO/IEC 27000 and SEI-CMMI as a method to conduct cybersecurity assessment and reporting. The answers were recorded, transcribed, and coded in a spreadsheet to elements of Rogers's diffusion of innovation theory using keywords aligned to Rogers's five-factors in an iterative process.

Table 8: Interview structure

Workshop Question #	**Section Header**	**Theory**	**Type**
1	Tell us about yourself	Demographics	3 point
2		Demographics	3 point multiple choice with Other
3		Demographics	5 point
4		Demographics	6 point multiple choice with other
5	This section of the survey explores the observability of interdependence of CI as an industry issue, the observability of it's impact on securing CI, and the observability of cyan-cmm as a solution	Observability	5 point likert
6		Observability	5 point likert
7		Observability	5 point likert
Talk about the model			
8	CMMs	Model	5 point likert
9		Model	5 point likert
10		Model	6 point multiple choice with other
11	Impact of Cybersecurity Capability Models	Trialability	5 point likert
12		Trialability	Open Text
13		Relative Advantage	5 point likert
14		Relative Advantage	5 point likert
15	This section of the survey explores the compatibility of the CMM to the current environment	Compatibility	5 point likert
16		Complexity or Simplicity	5 point likert
17	Implementation	Comments	Open text

In the second phase of the study a short cross-sectional web-based survey designed to quantitatively investigate the impact of the CMM on cybersecurity readiness was conducted inviting a large sample group to acquire the data. The survey instrument structure maps the questions to demographics required for the cluster analysis, and to the five factors of Rogers theory of Diffusion of Innovation. The questionnaire uses a combination of closed multiple-choice questions, closed scale questions, and open questions to draw the sample.

Table 9: Survey structure

Survey Question #	Section Header	Theory	Type
1	Tell us about yourself	Demographics	3 point
2		Demographics	3 point multiple choice with Other
3		Demographics	5 point
4		Demographics	6 point multiple choice with other
5	CMMs	Model	Yes/ No
6		Model	Yes/ No
7		Model	5 point likert
8		Model	5 point likert
9		Model	6 point multiple choice with other
10		Observability	5 point likert
11		Relative Advantage	5 point likert
12	Impact of Cybersecurity Capability Models	Trialability	5 point likert
13		Trialability	5 point likert
14		Compatibility	5 point likert
15		Relative Advantage	5 point likert
16		Complexity or Simplicity	5 point likert
17	Implementation	Observability	Yes, No, Don't know with comment
18		Comments	Open text

The Survey was hosted at Hostedincanadasurveys.ca on secure servers running the limesurvey tool in Canada. At the completion of the survey period data was deleted from the survey company server and is stored using AES256 encryption on secure servers located in Canada with

access restricted to the researchers. Respondents were also provided with the option of completing printable versions of the survey instrument and returning them via email or postal mail. Handwritten notes were transcribed and destroyed in order to preserve the anonymity of respondents.

Interview respondents were invited by references, and by their expression of interest through email. Interviews were conducted by telephone and in person at the convenience of the participant.

Respondents to the survey were invited through the Municipal Information Systems Association of Canada to legitimize the survey and foster participation. This was seen as a means of outreach to the population of municipal information technology practitioners, and as a means to minimize non-response bias. Directed invitations with telephone follow up were also sent using email to 170 participants. Many who responded were able to add legitimacy to the invitations by acting as references for the survey within their peer group and social network.

3.4 Data Analysis

The data analysis section describes how the data was analysed to produce the deliverables.

Member checking was used to validate accuracy of the interview findings through a review of the final report and specific parts back to the panel to determine its accuracy (Creswell, 2014:201).

Survey data was exported to Stata 13.1 in a UTF-16 comma separated value file for analysis. ANOVA tests and means comparison were used to identify the factors that affect model adoption

in municipalities and to determine the correlations and variances between the sample clusters.

Data on Size of municipality was obtained from the 2011 Census on municipalities produced by Statistics Canada. A cross-sectional web-based survey was used to collect data for the dependent and the other five independent variables (Creswell, 2014:164).

Statistical analysis using small sample analysis such as comparing means, Chi-squared tests, and analyses of variation (ANOVA) were performed to compare multiple variables with normal distributions for outcomes (Creswell, 2014:164).

3.5 Summary

This chapter has described the research method for this study by discussing the method, research design, data acquisition, and data analysis. This method and analysis results in a final version of the models being produced.

By triangulating the literature, expert responses, and the survey responses themes were derived for the results (Creswell, 2014:201).

By investigating how, why, and at what rates the Cybersecurity Capability Maturity model will spread through Canadian municipalities this study will de-risk the municipal technology manager's role in securing critical infrastructure and reduce both the cost and time to municipalities of deploying cybersecurity CMM compliance and reporting. The result being an improvement in cybersecurity and reporting of municipal Critical ICT infrastructure.

4 Results

Chapter 4 presents the results of the research study. It is organized into seven sections. Section 4.1 provides versions 1 and 2 of the CCMM. Section 4.2 describes versions 1 and 2 of the adoption model. Section 4.3 provides the questionnaire. Section 4.4 describes the sample. Section 4.5 provides the results of the ANOVA testing. Section 4.6 provides respondents' comments. Section 4.7 is a summary of the results.

4.1 Cybersecurity Capability Maturity Model (CCMM)

4.1.1 Version 1 of the CCMM

The CCMM is a methodology that can be used to develop and refine cybersecurity controls deployed in municipal critical infrastructure. Version 1 of the CCMM builds on existing and well accepted international standards. Version 1 conceptualizes the deployment of ISO/IEC 27000 controls as being assessed for maturity using the scoring based on SEI-CMMI. This scoring may be used as a benchmark against which to set improvement objectives and for the measurement and reporting of progress against the benchmark and objectives. The CCMM will provide municipal governments with a means to assess their current status with respect to prior assessments, identify realistic goals and priorities based on the metrics by ISO domain, and assess their current status in comparison with peer organizations or across industry sectors.

Table 10 provides version 1 of the CCMM.

Table 10: CCMM version 1

ISO 27000:2013 Security Domain	SEI CMMI Stage				
	1 Initiated	2 Managed	3 Defined	4 Quantitatively Managed	5 Optimizing
Process Maturity	Poorly controlled Unpredictable reactive	Characterized for each project Reactive	Proactive Characterized for Organization	Measured and Controlled	Focus is on improving
14 Domains of IT Security in ISO 27000					
Aggregate scores of sub-domains					

In CCMM version 1, controls are scored using CMMI like ratings as an aggregate score for each of ISO 27000's 14 security domains;

1. Information security policies
2. Organization of information security
3. Human resource security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operations security
9. Communications security
10. System acquisition, development and maintenance
11. Supplier relationships
12. Information security incident management
13. Information security aspects of business continuity management
14. Compliance (and law)

Assessment scores of the model reflect the aggregate maturity score of cybersecurity controls across interdependent CI's at the time of the assessment. These scores can be used as a baseline for comparison of future assessments to report progress over time.

4.1.2 Version 2 of the CCMM

Input on cybersecurity readiness assessment was taken from three experts from municipal government, critical infrastructure protection, and private cybersecurity practice in order to improve version 1 of the CCMM. The first expert consulted is a private cybersecurity consultant that has 32 years of related experience, and is CISSP-ISSAP, CISM, CRISC, TOGAF 9 and ITIL certified. The second expert consulted is a private cybersecurity consultant with over 20 years of experience, 15 years in critical infrastructure protection for a provincial emergency preparedness management organization. The third expert consulted is a current practitioner in a Canadian municipal IT security role, and who has 10 to 15 years of practical experience.

The experts agreed that municipalities are unique in that they operate multiple critical infrastructures. Asked about cybersecurity readiness, there was a consensus that municipalities are implementing tools for monitoring and protection, are reactive in their approach to incident management, and that current practices do not lend themselves to assess, report, and improve adoption over a time continuum. The municipal CI practitioner noted that the focus of municipal ICT operators is primarily on privacy legislation and payment industry obligations such as PCI-DSS and stated that many municipalities are out-tasking payment processing and health information management in order to ensure compliance where it is required, and insulate themselves from vulnerabilities and exploits.

The experts agreed that ISO/IEC 27000 is considered a valid and well known standard for

cybersecurity readiness. The critical infrastructure and private practice experts had good knowledge of available tools and offered that measuring maturity against well-known controls provides the best outcomes for operators. They were both aware of CMMI and agreed that it would be valuable in cybersecurity readiness assessment. They noted that ISO/IEC 27000 is complicated with 114 controls in 14 domains, and that efforts to simplify assessment such as providing specific guidance, and an easy to use comparison tool were important factors to incorporate in the model.

The experts suggested that improving the model with weighting of controls germane to the various critical infrastructure elements would guide implementers on the order of control implementation. Control weights will also allow flexibility in the models introduction providing a means for municipal CI operators to select controls tailored to their specific circumstances.

The CCMM for Canadian municipalities rates the implementation of controls (table 12) from the 14 security domains of ISO/IEC 27000:2013 (table 11) using SEI-CMMI like maturity scores from 1, initiated, to 5 optimizing. In the model each control in each domain is scored based on its maturity level, with the sum of the scores indicating the domains maturity level.

The scores can be used to ascertain the level of maturity at the time of the assessment, and to set goals for progression from this baseline to a desired future goal. These scores may be used to rate the municipalities relative ranking against all Canadian municipalities using a confidential index of aggregate scores.

Table 11: CCMM aggregate scoring

ISO 27000:2013 Security Domain	SEI CMMI Stage				
	1 Initiated	2 Managed	3 Defined	4 Quantitatively Managed	5 Optimizing
	Process Maturity				
	Poorly controlled Unpredictable reactive	Characterized for each project Reactive	Proactive Characterized for Organization	Measured and Controlled	Focus is on improving
Information security policies					
Organization of information security					
Human resource security					
Asset management					
Access control					
Cryptography					
Physical and environmental security					
Operations security					
Communications security					
System acquisition, development and maintenance					
Supplier relationships					
Information security incident management					
Information security aspects of business continuity management					
Compliance (and law)					

Of the 114 controls specified in ISO/IEC 27000:2013, our model sets an initial weighting of 79 as mandatory (2), and 35 as optional but important (1). Based on the weighting, municipalities will determine which controls fit with their environment.

Table 12: Weighting of controls in CCMM

No.	Control Name	Weight	No.	Control Name	Weight
5.1.1	Policies for information security	2	12.1.1	Documented operating procedures	2
5.1.2	Review of the policies for information security	2	12.1.2	Change Management	2
6.1.1	Information security roles and responsibilities	2	12.1.3	Capacity management	2
6.1.2	Segregation of duties	2	12.1.4	Separation of development, testing and operational environments	2
6.1.3	Contact with authorities	2	12.2.1	Controls against malware	2
6.1.4	Contact with special interest group	1	12.3.1	Information backup	2
6.1.5	Information security in project management	2	12.4.1	Event Logging	2
6.2.1	Mobile device policy	2	12.4.2	Protection of Log Information	2
6.2.2	Teleworking	2	12.4.3	Administrator and operator logs	2
7.1.1	Screening	2	12.4.4	Clock synchronisation	1
7.1.2	Terms and conditions of employment	2	12.5.1	Installation of software on operational systems	1
7.2.1	Management responsibilities	2	12.6.1	Management of technical vulnerabilities	2
7.2.2	Information security awareness, education and training	2	12.6.2	Restrictions on software installation	2
7.2.3	Disciplinary Process	1	12.7.1	Information systems audit controls	2
7.3.1	Termination or change of employment responsibilities	2	13.1.1	Network controls	2
8.1.1	Inventory of assets	2	13.1.2	Security of network service	2
8.1.2	Ownership of assets	1	13.1.3	Segregation in networks	2
8.1.3	Acceptable use of assets	2	13.2.1	Information transfer policies and procedures.	1
8.1.4	Return of assets	2	13.2.2	Agreements on information transfer	1
8.2.1	Classification of information	2	13.2.3	Electronic messaging	1
8.2.2	Labelling of information	2	13.2.4	Confidentiality or non-disclosure agreements	2
8.2.3	Handling of assets	2	14.1.1	Information security requirements analysis and specification	2
8.3.1	Management of removable media	2	14.1.2	Securing application services on public network	2
8.3.2	Disposal of Media	2	14.1.3	Protecting application services transactions	1
8.3.3	Physical media transfer	2	14.2.1	Secure development policy	1
9.1.1	Access control policy	2	14.2.2	System change control procedures	2
9.1.2	Access to Networks and network services	2	14.2.3	Technical review of applications after operating platform changes	1
9.2.1	User registration and de-registration	2	14.2.4	Restrictions on changes to software packages	1
9.2.2	User access provisioning	2	14.2.5	Secure system engineering principles	2
9.2.3	Management of privileged access rights	2	14.2.6	Secure development environment	1
9.2.4	Management of secret authentication information of users	2	14.2.7	Outsourced development	2
9.2.5	Review of user access rights	1	14.2.8	System security testing	1
9.2.6	Removal or adjustment of access rights	2	14.2.9	System acceptance testing	1
9.3.1	Use of secret authentication information	1	14.3.1	Protection of test data	1
9.4.1	Information access restriction	1	15.1.1	Information security policy for supplier relationships	2
9.4.2	Secure log-on procedures	2	15.1.2	Addressing security within supplier agreements	2
9.4.3	Password management system	1	15.1.3	Information and communication technology supply chain	2
9.4.4	Use of privileged utility programs	1	15.2.1	Monitoring and review of supplier services	1

9.4.5	Access control to program source code	2
10.1.1	Policy on the use of cryptographic controls	2
10.1.2	Key management	2
11.1.1	Physical security perimeter	2
11.1.2	Physical entry controls	2
11.1.3	Securing offices, rooms and facilities	2
11.1.4	Protecting against external and environmental threat	2
11.1.5	Working in secure areas	2
11.1.6	Delivery and loading areas	2
11.2.1	Equipment siting and protection	2
11.2.2	Supporting utilities	1
11.2.3	Cabling security	1
11.2.4	Equipment maintenance	2
11.2.5	Removal of assets	1
11.2.6	Security of equipment and assets off-premises	2
11.2.7	Secure disposal or re-use of equipment	1
11.2.8	Unattended user equipment	1
11.2.9	Clear desk and clear screen policy	1
15.2.2	Managing changes to supplier services	1
16.1.1	Responsibilities and procedures	2
16.1.2	Reporting information security events	2
16.1.3	Reporting information security weaknesses	2
16.1.4	Assessment of and decision on information security events	2
16.1.5	Response to information security incident	2
16.1.6	Learning from information security incidents	2
16.1.7	Collection of evidence	1
17.1.1	Planning information security continuity	1
17.1.2	Implementing information security continuity	1
17.1.3	Verify, review and evaluate information security continuity	1
17.2.1	Availability of information processing facilities	1
18.1.1	Identification of applicable legislation and contractual requirements	2
18.1.2	Intellectual property rights	2
18.1.3	Protection of records	2
18.1.4	Privacy and protection of personally identifiable information	2
18.1.5	Regulation of cryptographic controls	1
18.2.1	Independent review of information security	2
18.2.2	Compliance with security policies and standards	2
18.2.3	Technical compliance review	2

4.2 Adoption model of the CCMM

4.2.1 Version 1 of the Adoption model of the CCMM

Version 1 of the adoption model focused on leveraging Rogers' diffusion of innovation model to spread the CCMM through municipalities across Canada.

Figure 2 illustrates version 1 of the adoption model. This model is a process comprised of four steps:

1. Researchers provide input to:
    a. An open source model for the implementation, assessment, and reporting of cybersecurity controls in municipal critical infrastructure
    b. Exploits and vulnerabilities in the domain
2. A respected standards organization and / or institute
    a. Legitimizes the model

b. Provides collateral and training on the model, assessment, and reporting

3. Gatekeepers or innovators
    a. Share their experience with cybersecurity CMM's to diffuse the model to early adopters
    b. Provide critical feedback for the improvement of the model
4. Opinion leaders and the early adopters
    a. Share their experience with others in their peer group
    b. Provide critical feedback for the improvement of the model

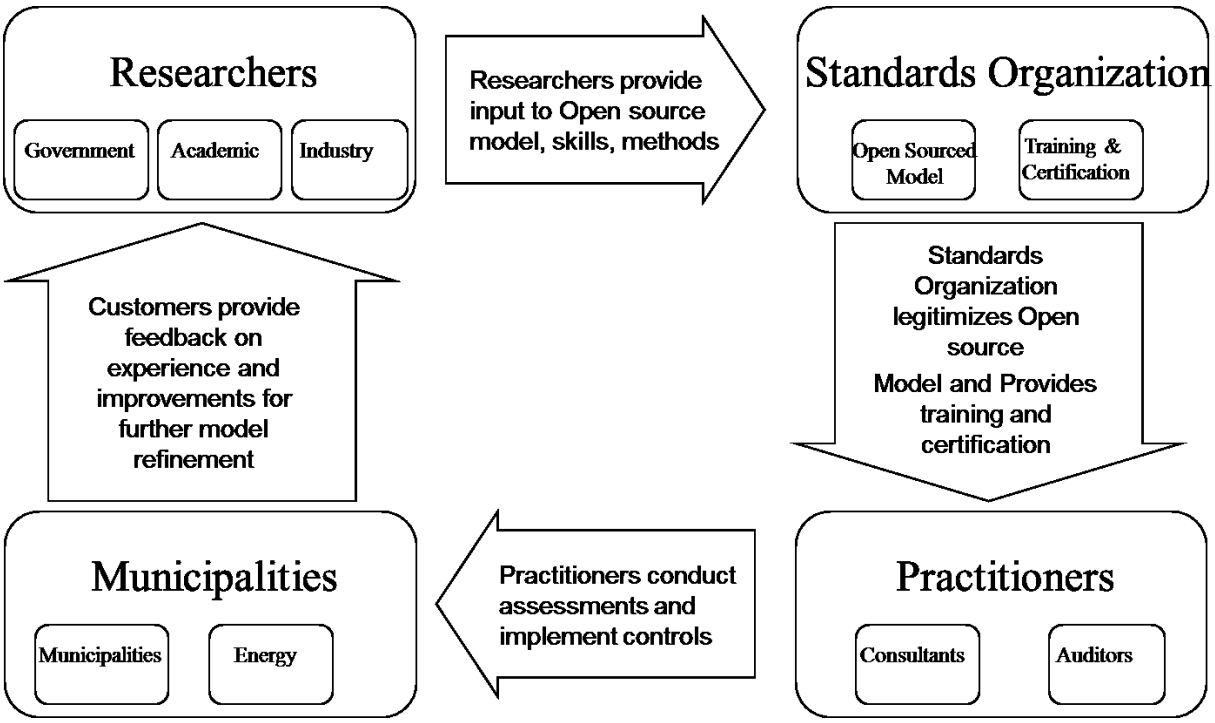

Figure 2: Version 1 of the Diffusion Model for CCMM

.

4.2.2 Version 2 of the Adoption model of the CCMM

Feedback was solicited from the expert panel regarding version 1 of the adoption model. Their experience with municipal CI operators shows that decision makers in the municipalities are neither IT nor Security experts. They indicated that improving the observability of the importance of regular cybersecurity readiness assessment and tools for that purpose at the City

Clerk/Manager, Chief Administrative Officer, CSO, and CEO levels is the most important factor to consider in order to diffuse the model and gain supports for improving readiness. The primary benefit of improving observability of the model at this level would be to:

- Assess current readiness and set objectives for improvement
- Gain support for human resources
- Gain support for financial resources
- Report progress on objectives

Considering the diffusion model, the experts identified ease of use of the CCMM as the next most important factor for consideration. While compatibility with process and systems is important, they felt that a CCMM for municipal CI would be new to the environment and therefore not constrained by existing practices. Low observability of CMMs by municipal CI operators including CMMI was identified as a concern by the expert panel and they suggested that demonstrating performance of the CCMM through workshops, peer reviews, and a confidential ranking system as ways to improve observability. They did express that the energy industry has more experience with maturity modeling relative to CI protection, though they were unsure if this experience would be exploited as many municipalities are divesting of their energy assets.

Finally, the experts cautioned that cybersecurity data is generally exchanged between agencies and is seldom shared externally, therefore gaining support for the study and subsequent sharing of CCMM scoring would prove difficult. They made two recommendations:

1. A trusted party such as MISA be used as a sponsor for the study and workshops
2. That regulatory oversight be used to promote adoption.

Figure 3 illustrates version 2 of the Diffusion Model for the CCMM which is an iterative process comprised of four steps. These steps are:

1. Researchers provide input to:
    a. An open source model for the implementation, assessment, and reporting of cybersecurity controls in municipal critical infrastructure
    b. Exploits and vulnerabilities in the domain
2. A respected standards organization and / or institute
    a. Legitimizes the model
    b. Validates performance of the model
    c. Provides collateral and training on the model, assessment, and reporting
    d. Provides a confidential ranking index for Canadian municipalities to assess their relative position in their peer group
3. Gatekeepers or Innovators
    a. Share their experience with cybersecurity CMM's to diffuse the model to early adopters
    b. Provide critical feedback for the improvement of the model
    c. Share their assessment in the confidential ranking index
4. Opinion leaders in the early adopters
    a. Share their experience with others in their peer group
    b. Provide critical feedback for the improvement of the model
    c. Share their assessment in the confidential ranking index

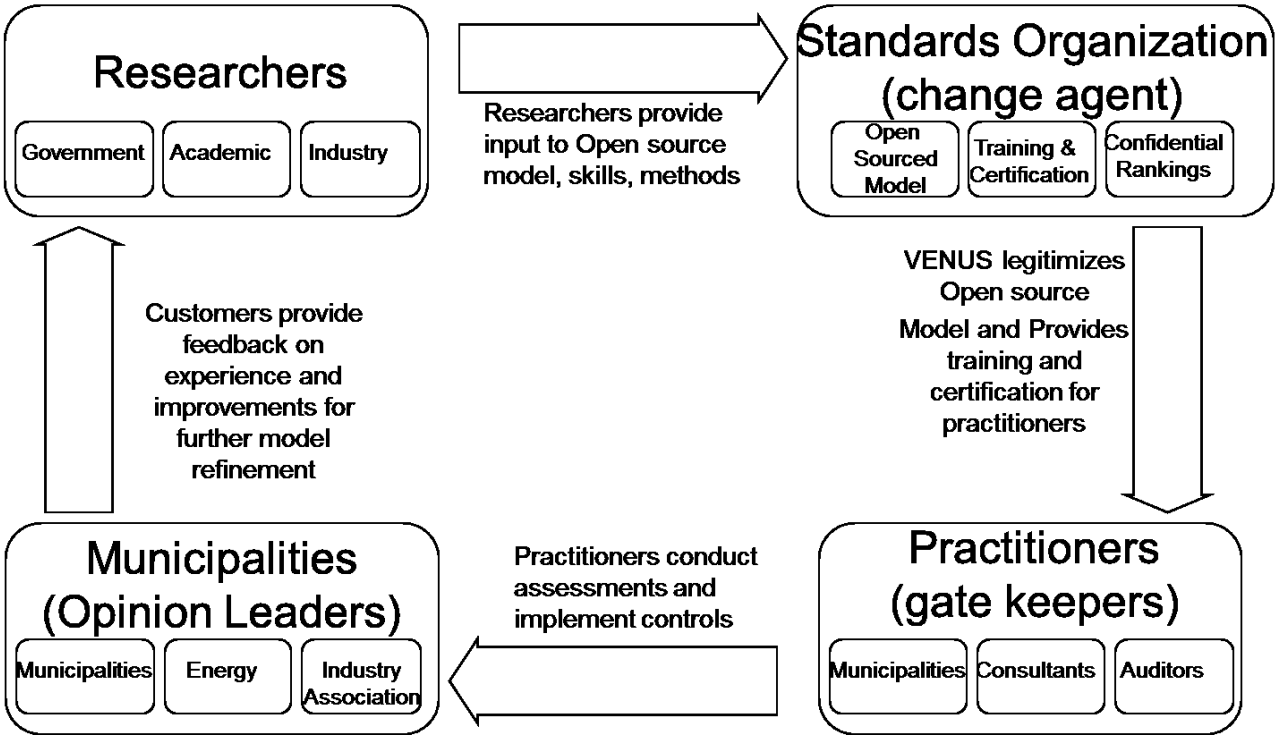

Figure 3: Version 2 of the Diffusion Model for CMM

For each actor in the model, Table 13 describes its role and deliverables.

Table 13: Actors and roles in diffusion model

Actor	Role	Deliverables
Researcher	Input to vulnerabilities, exploits, Models, Skills, Methods	• Academic research • Models • Proofs
Standards Organization / Institute	Provide ability and motivation (Impetus for change)	• Legitimacy for models • Standards collateral • Training • Ranking index
Gate Keepers	Provide heterophily (knowledge of the innovation) to balance group behavior	• Share experience with opinion leaders • Input to model refinements
Opinion Leaders	Act as "*champions*" in the organization to promote the innovation	• Share experience with practitioners, management • Input to model refinements
Homophilous Group of practitioners	Promotes diffusion among each other	• Share experience with Group • Input to model refinements

Table 14 identifies the consequences of Model Diffusion.

Table 14: Consequences of Model Diffusion by public and private sectors

	Consequences	
Undesirable	• Loss of data • Cascade failure • Loss of service • Economic Impact	• Regulatory Sanctions • Media reports of vulnerability or exploit • Loss of position
Desirable	• Security of data • Quality of services • Positive economic result • Security of assets and constituents	• Positive recognition • Resources for improvement • Reduced risk • Job security
	Public	Private

It is estimated that the 2.5% of municipalities that are currently using ISO/IEC 27000 are innovators and trusted advisors. These municipalities can be used to refine the CCMM provided in this study and promote its use. We can also consider those municipalities with high ISO/IEC 27000 and CMMI observability, and regular assessment execution scores as potential early adopters and leverage their experience with the model. We can build legitimacy of the model through a respected institute such as VENUS Cybersecurity Corporation and leverage trusted sources such as MISA and Public Safety Canada, to act as change agents, improve observability of the problem space and model to inform decision makers in Canadian municipalities.

4.3 Questionnaire

4.3.1 Version 1 of the questionnaire

The study utilized an 18 question, web-based, survey. The survey is provided as Appendix A. The survey instrument was divided into six sections; an introduction page, demographic questions, CCMM questions, Impacts of CCMM questions, Implementation question, and finally a conclusion page.

The introduction page introduced the study, provided links to background material, indicated the

time using a range of 10 to 15 minutes, indicated the respondent's rights and how the data would be treated anonymously, and concluded with contact information for the researchers and ethics board members. The introduction was a one and a half pages in length.

The next four sections of the survey were comprised of multiple choice closed questions as well as open ended questions collecting data on the demographics of the respondents, their knowledge of CMM's and cybersecurity protocols, which factors would impact CCMM adoption, and other feedback. Each question provided a neutral response option, as well as an-opt out option.
The final page of the survey thanked the respondent, offered them contact information to provide follow up information, and allowed them to submit their response.

4.3.2 Version 2 of the questionnaire

The survey instrument was reviewed by an expert with over 20 years of experience in management, and survey research. This resource was separate from those consulted for their expertise on critical infrastructure protection and the CCMM and adoption models. Positive feedback was received about the overall length and structure of the survey as well as the link to background material and rationale for asking the questions. Several suggestions were made to improve the survey response rate. First, it was noted that the introduction page was unnecessarily lengthy. It was recommended that the text be shortened to reduce the reading and time required of the respondent. Second, it was recommended to plainly state the time required to complete the survey rather than providing a range. Next, it was noted that the text on participant anonymity and data encryption was lengthy and could influence respondents to abandon the survey, and a recommendation was made to make this text more concise. Finally, feedback was provided that response rates of web-based surveys are lower than paper based surveys and a recommendation was made to allow respondents the alternative to return printed versions by email, postal mail, and facsimile as well as online.

Feedback from the consultant was included in version 2 of the survey (appendix B). First, the introduction page was shortened to one page, retaining the introduction, links to background information and an edited version of the data protection paragraph. The contact information was moved to the final page of the survey. Next, survey completion was timed with test cases and the corresponding statement edited to reflect the actual time of under five minutes. Finally, respondents were provided with the option of using email and postal mail as alternatives to completing the survey online.

4.4 Sample

This study has a confidence level of 80% and a confidence interval (margin of error) of ± 9.96, therefore data in these results is expected to be correct within plus or minus 9.96 eighty percent of the time. A sample of 42 survey responses was taken from the population of Canadian Municipal governments, which the 2011 Canadian census states as 4,748. Using the population (N), the sample size (n), and a response distribution of 50%, the confidence level and interval were calculated.

Respondents were required to submit their responses as a mechanism for gaining consent to use the data. In this process, 14 (21%) respondents chose to abandon their survey after completing all questions. The survey experienced higher than anticipated non-response bias despite the methods designed into the survey to minimize it. Initially, the survey respondents were invited through a posting on the MISA member's website and through communications to their members by the MISA executive. Reminder messages were sent to members periodically. When the response rate did not improve, directed email invitations were made to potential respondents using their email addresses where they were known, and through general inquiry email addresses and web pages

of the municipalities. Subsequent to the email campaign, telephone follow up to potential respondents were conducted. Where contact was made directly, requests were made to be refereed to other municipal IT peers. Each of these campaigns had corresponding peaks in survey responses. When no further contacts were possible and incremental responses ceased, the survey was terminated. A larger sample size would have improved the confidence level and confidence interval of the study. Nevertheless, the sample is satisfactory for statistical analysis using small sample analysis such as comparing means, Chi-squared tests and ANOVA testing.

The first section of the survey collected data on the demographic constitution of the sample with the intent to determine whether population size, role and experience of respondent, and the types of critical infrastructures operated impacted the survey data.

The survey sample consisted of 5 (12%) small municipalities with populations of less than 10,000, (30) 72.5% medium municipalities with populations of between10, 000 and 500,000, and 3 (7%) large municipalities with populations greater than 500,000 constituents. 3 (7%) respondents did not specify the size of their municipality.

The survey targeted information technology management and this is represented in the results with roughly 34 (85%) respondents in management and senior management roles. 2 (4.7%) described themselves as cybersecurity experts, and 4 (9.5%) described themselves in other roles. Experience levels were distributed amongst the categories with little variation. 8 (19%) respondents have 1 to 5 years of industry experience, 8 (19%) respondents have 5 to 10 years of experience, 8 (19%) respondents have 10 to 15 years of experience, and 7 (17%) respondents have greater than 10 years of experience. 11 (26%) respondents did not specify their experience level.

Survey participants were asked to choose from a list of 6 critical infrastructure categories and were allowed to enter other categories if applicable in order to determine which were operated by Canadian municipalities. The results show that 4 (9.5%) operate electricity, 24 (57%) operate water, 18 (42.8%) operate transportation control, 24 (69%) operate emergency services and public safety, 25 (59.5%) operate municipal information and communications technology, and 21 (50%) operate eGovernment and constituent data systems. Of the respondents, only 3 (7.1%) did not operate multiple critical infrastructures. This supports our assertion that Canadian municipal operators of critical infrastructure constitute a unique category of operator.

4.5 Results of the ANOVA testing

4.5.1 Results of ANOVA testing of observability

Questions were posed to survey participants to understand the observability, or common understanding, of both the problem space of cybersecurity readiness assessment and of tools available for this purpose.

Respondents were asked about the importance of regular cybersecurity assessment using a 5 point Likert scale with strongly agree equal to 5 and strongly disagree equal to 1. 31 (73.8%) respondents supported the statement by choosing agree or strongly agree as a response. Responses to the question were compared using the role and experience of the respondents and municipal population size to determine if sub-groups viewed the importance of regular cybersecurity readiness differently using one-way ANOVA tests. Little variation was observed across the municipal sizes, with small municipalities with the lowest score (M=3.75), and medium (M=4.148) and large (M=4.3) showing agreement. There was also little variation between experience levels of respondents with all agreeing or strongly agreeing that regular assessment is important. However, there was a significant effect of respondents with different roles, C-level executive, IT manager, cybersecurity expert, and other, on the importance of regular assessment at the $p<.05$ level for the four conditions [$F(3, 32) = 4.15$, $p = 0.0137$]. The

mean score for the C-level executive role (M=3.571, SD=0.787) was lower than the IT manager role (M=4.347, SD=0.572) and cybersecurity expert (M=5, SD=0). Taken together, these results suggest that the importance of regular cybersecurity readiness assessment is consistent across practitioners of varying experience level and municipal sizes, but is lower at the executive level.

The survey measures the frequency of cybersecurity assessment in municipal CI providers in question 11 which indicates that assessment is occurring roughly every twelve months (M=3.7). Of this group 27 (64.2%) are conducting regular readiness assessments, and only 3 (7.1%) participants stated that they do not regularly assess their cybersecurity readiness. This result shows that 10% fewer municipalities are performing regular assessment than supported its importance.

Respondents were asked whether they were knowledgeable about ISO/IEC 27000, with an answer of yes equal to 1, and no equal to 2. The responses indicate low observability or awareness of ISO/IEC 27000 (M=1.66) in the sample. Stated differently only 10 (23.8%) respondents had knowledge of ISO/27000. A one-way ANOVA test was conducted comparing the effect of municipal population on practitioner ISO27000 knowledge. There was a significant effect of the population size on ISO27000 observability at the $p<.05$ level for the three conditions [$F(2,33) = 4.47$, $p = 0.0191$]. Small municipalities reported no knowledge of the protocol (M=2, SD=0) and medium (M=1.75, SD=0.435) and large (M=1, SD=0) municipalities reported knowledge of ISO27000. Of the 7 respondents with knowledge of ISO 27000 6 are performing regular readiness assessments. Taken together these results suggest that knowledge of ISO27000 is low overall, with higher concentration in large and medium municipalities.

Respondents were asked whether they were knowledgeable about SEI-CMMI with an answer of yes equal to 1, and no equal to 2. The responses indicate that observability of SEI-CMMI as a

tool for cybersecurity capability maturity modelling is low (M=1.833). 4 (9.5%) respondents stated that they were knowledgeable about CMMI and these positive responses relating to CMMI were found in the large and medium municipalities. 3 of the 4 respondents responding that they were aware of CMMI are performing regular cybersecurity assessment. These results suggest that observability of SEI-CMMI is low overall, with higher concentrations in large and medium municipalities. They also suggest a correlation between observability of the tools and conducting regular cybersecurity assessment.

Survey participants were asked to identify any capability maturity models that they were using in their assessment of cybersecurity readiness. Of the seven potential options provided; SEI-CMMI, SSE-CMM, C2M2, ES-C2M2, ONG-C2M2, "I do not use a model", and "other", 38 (90.5%) respondents stated that they do not use a CMM for this purpose. 1 (2.5%) respondent stated that they use ISO/IEC 27000 for this purpose. From this result we observe that capability maturity models are not used for cybersecurity readiness assessment in Canadian municipalities.

Asked the question, "would a confidential index plotting your maturity level relative to peer organizations aid in promoting cybersecurity readiness?" respondents were generally supportive of using a confidential ranking index as an aid with 22 (52%) responding yes. Their verbatim comments (appendix D, table 18) state that such a tool would be useful in setting an impetus for change as well as in gaining direction, and human and financial resources for improving cybersecurity readiness. Support for the tool is stronger in the larger municipalities, and somewhat so in the mid-tier municipalities.

4.5.4 Results of ANOVA testing of factors impacting model adoption

Respondents were asked using a five point Likert scale with strongly agree equal to 5 and strongly disagree equal to 1 whether the ease of use of a cybersecurity capability maturity model

is a factor in its adoption. 18 (42.8%) respondents answered that they agree or strongly agree that simplicity of the model is important to its adoption. One-way ANOVA tests were conducted comparing the effect of municipal size and respondent experience on the importance of simplicity of the CCMM to its adoption. Results show that there is little variation in the responses between the municipal sizes. There was a significant effect of respondent experience on model simplicity at the $p<.05$ level for the four conditions [$F(3, 23) = 4.32$, $p = 0.0149$]. Respondents with greater than 15 years' experience (M=3.32, SD=0.447) and those with 1 to 5 years' experience (M=3.5, SD=0.756) found it less important than those with 5 to 10 years' experience (M=4.428, SD=0.787), and 10 to 15 years' experience (M=4.286, SD=0.756). Taken together, these results suggest that the importance of model simplicity is consistent across municipal sizes, but varies with the experience level of the respondent with simplicity most valued by practitioners with 5 to 15 years of experience. Table 15 shows the ANOVA results comparing the importance of model simplicity by respondent experience.

Table 15: Value of simplicity of model by respondent experience

. oneway simp3 exp, tabulate

Summary of Simp3

EXP	Mean	Std. Dev.	Freq
A2	3.5	0.75592895	8
A3	4.428571	0.78679579	7
A4	4.285714	0.75592895	7
A5	3.2	0.4472136	5
Total	3.888889	0.84731855	27

Analysis of Variance

Source	SS	df	MS	F	Prob > F
Between groups	6.72380952	3	2.24126984	4.32	0.0149
Within groups	11.9428571	23	0.519254658		
Total	18.6666667	26	0.717948718		

Bartlett's test for equal variances: chi2(3) = 1.4099 Prob>chi2 = 0.703

Respondents were asked if the ability to trial or test cybersecurity readiness improvements using a model prior to formal adoption would increase the adoption of the model with a five point

Likert scale with strongly agree equal to 5 and strongly disagree equal to 1. 28 (66.6%) respondents stated that they agreed or strongly agreed that trialability is beneficial to model adoption. 2 (4.7%) stated that they disagreed with this statement. 5 (11.9%) stated that they did not know. A one-way ANOVA test was conducted comparing the effect of respondent role on the importance of triability of the CCMM. There was a significant effect of respondent role on model trialability at the $p<.05$ level for the four conditions [$F(3, 31) = 1.83$, $p = 0.163$]. The mean score for the C-level executive role (M=3.5, SD=0.926) was lower than the IT manager role (M=4.143, SD=0.727) and cybersecurity expert (M=4.5, SD=0.707). Taken together, these results suggest that the importance of model trialability is higher with practitioners than at the executive level. Table 16 shows the ANOVA results comparing the importance of model triability by respondent role.

Table 16: Value of trialability of model by respondent role

. oneway trial1 rol, tabulate

Summary of Trial1

EXP	Mean	Std. Dev.	Freq
A1	3.5	0.9258201	8
A2	4.142857	0.72702918	21
A3	4.5	0.70710678	2
A4	3.75	0.5	4
Total	3.971429	0.78537044	35

Analysis of Variance

Source	SS	df	MS	F	Prob > F
Between groups	3.15	3	1.05	1.83	0.1629
Within groups	17.8214286	31	0.574884793		
Total	20.9714286	34	0.616806723		

Bartlett's test for equal variances: chi2(3) = 1.3049 Prob>chi2 = 0.728

Questions 13 and 14 investigated the improvement in model adoption time influenced by trialability of a model prior to formal adoption, and a model being compatible with their existing environment. Question 15 investigated the perceived improvements in conducting cybersecurity readiness assessments using a cybersecurity capability maturity model. Missing data in these three variables impacted their confidence levels. In each of the cases there was weak support for

improvement in assessment using a CCMM that is easy to use and able to be tested prior to formal adoption.

4.6 Comments from respondents

At the end of the survey, respondents were given the opportunity to add additional comments and insight to aid the researchers. Verbatim can be found in appendix D.

Many of the comments supported the use of a confidential index ranking municipalities on their maturity that could be used to garner direction, and human and financial support, or to track improvement.

Another interesting comment supported the expert assertion that agency to agency interaction is a viable vector for engaging the municipalities, in this case suggesting that the Municipal Information Systems Association of Canada could be a partner in the efforts, "Your assumption is that each municipal organization is doing this independently. Not the case. We need a coordinated approach through an org like MISA-ASIM Canada."

Common themes supporting improvement in education and awareness also surfaced in the verbatim that support the low observability scores in the survey.

4.7 Summary of results

This study drew a sample of 42 completed responses from a population of 4748 Canadian municipalities. 10 (23.8%) respondents were senior managers and 24 (57.1%) were IT managers. The municipalities confirmed that they operate multiple critical infrastructures though only four included Energy.

Observability of the problem space is high. 31 (73.8%) respondents supported that regular cybersecurity assessment is important to their organizations. The executive levels, while seeing this as important, show less support than managers and subject matter experts. Assessment is taking place on average every twelve months but there is room for improvement. 27 (64.2%) respondents stated that they regularly assess readiness, and 3 (7.1%) stated that they never assess cybersecurity readiness.

Observability of tools for cybersecurity capability maturity modelling such as ISO 27000 and CMMI is low. Only 10 (23.8%) respondents stated that they were knowledgeable about ISO/IEC 27000 and just 4 (9.5%) respondents stated that they were knowledgeable about CMMI. This support is shown entirely in the large and mid-tier municipalities. Of those that state knowledge of ISO/IEC 27000 and / or CMMI, all were conducting regular readiness assessments. Only 1 (2.4%) stated that they were using ISO 27000 for readiness assessment. No other cybersecurity capability maturity models were in use.

Survey verbatim suggest that demonstrating the performance of the CMM would aid practitioners in their decision and this is supported by the survey result of 28 (66.6%) stating that trialability would aid in model adoption.

22 (52.4%) survey participants responded that a confidential Index ranking them against the industry would aid in adoption of the model and improving cybersecurity readiness. Respondents stated that they would use such a tool to secure the necessary financial and human supports required to improve cybersecurity readiness.

The relative advantage of the model was positive in interviews with experts. There was weak support for an improvement in readiness assessment in the survey. Responses indicate that model

adoption would improve by 6 months if the model were compatible with existing methods. However, due to missing data and neutral responses in the variables designed to determine the advantage of the CCMM it is not possible to predict with precision the model adoption rate or improvement in readiness assessment time.

5 Discussion of Results

Chapter five relates the results with the research question and objectives. It is organized into four sections. The first section discusses municipal critical infrastructure. The second section discusses cybersecurity and cybersecurity capability maturity models and the development of the cybersecurity maturity model delivered in this research. The third section discusses potential adoption approaches. The fourth section is a summary.

5.1 Municipal Critical Infrastructure

Municipalities form a unique category of operator due to their deployment and operation of multiple interdependent networks of critical infrastructure. This interdependence shown in figure 2 places municipalities at increased risk of cascading failures (Bukdyrev et al., 2010; Vespignani, 2010) and requires attention to their design for resiliency and security (Xiao-Juan & Li-Zhen, 2010; Rahman et al., 2011). The interview portion of the study determined that there is awareness of the interdependence and design challenges that it poses with cybersecurity experts and emergency management planners, and to a lesser extent in the municipal IT practitioners. The study confirms that municipalities consistently operate combinations of electrical, water, transportation control, emergency services /public safety, eGovernment, and information and communications technology assets.

5.2 Cybersecurity Capability Maturity Models

Capability maturity modelling has its roots in improving quality in software engineering (Wendler, 2012). Applied to cybersecurity readiness assessment maturity modelling has been introduced in different security frameworks in various forms (Table 4) that aim to move practitioners towards set goals. In terms of Canadian municipal critical infrastructure operators, none

have adopted any of the models presented for readiness maturity assessment. 2.5% (1 operator in our study) indicated that they use ISO/IEC 27000 for assessment however ISO 27000 does not perform maturity modelling. The responses show that observability of ISO/IEC 27000 and SEI-CMMI are low in Canadian municipal CI operators, and within this domain they are better known at the practitioner level than the executive levels. This explains in part why adoptions of CMM's are low. There is an opportunity to work with the municipalities to improve the observability of CMM's for cybersecurity readiness assessment and to develop a model germane to their domain.

Discussion of cybersecurity capability maturity model development

A cybersecurity capability maturity model was developed and refined in consultation with industry experts in the first two steps of the research method. The model is comprised of elements of ISO/IEC 27000 (27001:2013, 27002). It was determined in the first phase of the study that a legitimized model can only be realized using international cybersecurity standards developed by a credible institution. ISO/IEC 27000 is comprehensive, current, and with the addition of incremental controls could meet the needs of Canadian Municipalities operating interdependent CI.

Scoring of maturity of control implementation was identified as a necessity of the model as current practices are typically binary in nature, do not assess against target goals, and are difficult, time consuming, and expensive to implement leading organizations to implement subsets of a standard like ISO 27000. Weighting of controls was also identified as a requirement of a model as not all 114 ISO27000 controls are applicable to this domain, and additional controls missing from ISO27000 may be required.

5.3 Diffusion model

In conducting this study several artifacts of investigating cybersecurity practices were encountered. In order to address potential non-response bias, efforts were taken to add legitimacy to the study such as sponsorship by Carleton University and Public Works and Government Services Canada, highlighting the scrutiny and approval of the university research ethics board, and the approval of the Board of Directors of the Municipal Information Systems Association of Canada. Despite these efforts the study experienced lower than anticipated response rates and we learned that it is difficult to engage cybersecurity subject matter experts without being referenced to them through their network. In many cases during data collection, responses came more quickly when direction was given by senior management that participation was approved. This is supported by input from the expert panel in the first phase of the study that support for model implementation would be needed by senior management as the biggest single challenge will be direction.

The diffusion model developed and refined in the study (chapter 4.2) applies the learnings of this study with diffusion of innovation theory to build a plan for model adoption.

A tension for change is required to foster the adoption of cybersecurity capability maturity models in Canadian municipal critical infrastructure providers. The survey scores testing perception of the need for regular assessment indicate that 75% agree. However, only 65% are performing assessment, and only 2.5% are using a tool such as ISO/IEC 27000. In the interview portion of the study, respondents indicated that they had out-tasked functions such as payment processing, medical recording for long-term care and emergency medical services, and website hosting in order to meet privacy regulation, payment compliance requirements, and to insulate themselves from cybersecurity exploits. This indicates that the consequences of not acting in these domains has served as the impetus for action to secure these assets. Regulation, improving

observability of the consequences of not acting, and initiatives led by associations are possible tensions for change for municipal CI operators. Survey verbatim indicated that MISA is an avenue for leading collaboration in Canadian municipalities. Regardless, we conclude that regular assessment and reporting of critical infrastructure elements will be mandated through regulation or the legal consequences of inaction.

Decision making in organizations is categorized into consensus and authoritative. The adoption of cybersecurity capability maturity models for cybersecurity assessment will require direction and support from senior management of Canadian municipalities. Our study indicated that observability of the importance of regular assessment is lower in the executive levels than with practitioners. The study also indicated that over 51% of respondents desire a confidential ranking tool that they would use to compare their readiness and as a tool to gain financial and human resources from their executive. The adoption of a CCMM will also need the support of the municipal CI community using an external influence with knowledge of cybersecurity capability maturity models. In our diffusion model, we consider the 2.5% that are currently using ISO/IEC 27000 as the innovators and trusted advisors because the survey results indicate that they have high observability of CMM's and are conducting regular cybersecurity assessments using the ISO model. We consider those with high ISO/IEC 27000 and CMMI observability, and regular assessment execution scores as potential early adopters, and we leverage their experience with the model. We consider respected institutes like the VENUS Cybersecurity Corporation, the Municipal Information Systems Association, and Public Safety Canada as trusted sources to build legitimacy and inform decision makers.

5.4 Summary

This chapter related the results of our research in developing a Cybersecurity Capability Maturity Model (CCMM) for Canadian municipalities and to provide recommendations on the adoption of

such a model. The first section discusses municipal critical infrastructure and why it can be considered a unique category of critical infrastructure. The second section discusses cybersecurity capability maturity models, their lack of adoption in Canadian municipal CI operators, and the development of the cybersecurity maturity model delivered in this research. The third section discusses how the CCMM would diffuse through Canadian municipal CI operators and the development of the diffusion model delivered in this research.

6 Conclusions

Chapter six is organized into five sections. The first section presents the conclusions of the research. The second section discusses the contribution to policy of the thesis. The third section discusses the contribution to engineering management practitioners. The fourth section discusses the limitations of the research, and the fifth section presents suggestions for future research.

6.1 Conclusions

The objective of this study was to investigate how, why, and at what rate a Cybersecurity Capability Maturity Model (CCMM) will spread through Canadian municipalities, to develop such a CCMM for Canadian municipalities, and to develop a model for the adoption of such a CCMM in Canadian municipalities.

Improving observability of critical infrastructure dependencies and CCMM's will aid in model adoption. Cybersecurity capability maturity modeling is not in use in Canadian municipalities. Low observability of CMM's and cybersecurity CMM's was indicated in the survey and there is a correlation between observability of the models and regular cybersecurity assessment. Finally, the study provides data on the observability and sentiment of cybersecurity assessment across management tiers and municipal sizes in Canadian municipal CI operators, and highlights the need for improved observability of these topics in senior management levels. Therefore, improving observability at the municipal executive level is a priority to improve model adoption.

Ease of trialability of the CCMM and its use improves model adoption. There was support that the ability to demonstrate performance of the model prior to formal adoption in an organization would improve its adoption. Demonstrating the performance of a CCMM to practitioners with

knowledge of the tools would result in a pool of potential early adopters who could aid in its diffusion through Canadian municipalities.

Increasing the simplicity of the CCMM implementation and use improves model adoption. There is support in the results that the simplicity of the model impacts its adoption.

Compatibility of the model with existing methods is not important for model adoption as CCMMs are new to Canadian municipal CI protection.

Combining ISO/IEC 27000 controls, SEI-CMMI maturity scoring, and weighting of controls provides a simple cybersecurity capability maturity model that provides guidance on securing this complex system with relative advantage over current reactive methods.

As municipal CI operators do not have the acumen or resources to address implementing CCMMs for CI cybersecurity improvements an opportunity exists to build a market for the supply of these tools and resources in order to quickly address this gap.

6.2 Contributions to Policy

This study illustrates a gap in the policy on critical infrastructure cybersecurity. While the importance of cybersecurity readiness assessment was consistent across the municipalities with 75% claiming that it is important, just 65% are conducting regular readiness assessments, and none are using CCMMs for these assessments, despite the cooperative frameworks for CI protection in place in Canada. Without a tension for change model adoption in organizations will be difficult to cultivate. Guidelines for a minimum level of cybersecurity protection for municipal critical infrastructure are required, similar to the national building code (NBC). Survey respondents indicated that using a confidential rating index ranking their cybersecurity readiness

maturity against other municipalities would be useful in gaining support of executives for human and financial resources. They also indicated that privacy and financial compliance policy served as an impetus for out tasking payment and medical recording systems to ensure their security. Combining a mandated minimum level of cybersecurity protection for critical infrastructure such as maintaining a minimum maturity level with reporting is a prudent approach for critical infrastructure protection.

6.3 Contributions to Engineering Management Practitioners

This study contributes to engineering management practitioners in four ways.

First, the study provides data on the type and mix of critical infrastructure operated by Canadian municipal operators, confirming that it is common practice to operate multiple critical infrastructures. Understanding this factor will aid the development of better models for cybersecurity protection in Canadian municipal operators.

Second, the study provides data on the current use of CCMM's for cybersecurity assessment and protection in Canadian municipal operators, determining that they are not widely used, and highlighting the need for further efforts to promote adoption of CCMM's in cybersecurity readiness assessments.

Third, the study provides the first iteration of a CCMM for Canadian municipal critical infrastructure providers based on ISO/IEC 27000 to inform controls and SEI-CMMI to inform maturity scoring for cybersecurity readiness. In doing so, the study lays a foundation for improving the assessment, security, and reporting of Canadian municipal critical infrastructure.

Finally, the study contributes an initial diffusion model for the CCMM in Canadian municipalities in order to encourage the adoption of CMM's for cybersecurity readiness assessment and reporting.

6.4 Limitations

In conducting this research at least four limitations were identified.

First, despite efforts to mitigate for biases such as adding legitimacy through the University, MISA, references, and Public Works and Government Services Canada, the survey had a low response rate impacting confidence levels, and exposing the survey to potential non-response bias.

Second, cybersecurity readiness is a complex and sensitive topic. While background information was provided to survey respondents, anonymity and security of data was assured, and opt out choice provided for survey questions, there is a potential response bias associated with this topic through ignorance of CMM's or an inability or unwillingness to share data.

Third, due to the low response rate and low observability of cybersecurity maturity models, answers to questions intended to quantify the perceived relative advantage of the CMM developed in the study resulted in low statistical power. Therefore we cannot state relative advantage of the model with confidence.

Fourth, the performance of the cybersecurity capability maturity model developed in this study has not been tested empirically.

6.5 Future Research

Five topics are identified for potential future study.

First, investigating the impact of the weighting of specific controls from the CCMM on various use cases would improve the model, allowing specific guidance for various combinations of critical infrastructures operated by municipalities.

Second, this cross sectional study may be validated with a larger sample size in order to improve confidence levels of the results.

Third, a longitudinal study of the impact of cybersecurity capability maturity model adoption on cybersecurity readiness assessment and reporting would inform decision makers of the advantage of this method.

Fourth, the model identified in this study can be tested for performance which can then be used to inform decision makers in federal, provincial, and municipal governments, and in industry associations.

Finally, business models for the supply of the CCMM can be explored.

7 References

Academy of Management Review. 2007. Style guide for authors. 32(1): 313-316. http://www.aom.pace.edu/amr/AMRstyleguide.pdf

Adams, M., Makramalla, M., & Miron, W. n.d. ***Down the Rabbit Hole: How Structural Holes in Entrepreneurs' Social Networks Impact Early Venture Growth***. http://timreview.ca/sites/default/files/article_PDF/Adams_et_al_TIMReview_September2014.pdf, September 29, 2014.

Agresti, W. W. 2010. The four forces shaping cybersecurity. ***Computer***, 43(2): 101–104.

Andersen, K. V., & Henriksen, H. Z. 2006. E-government maturity models: Extension of the Layne and Lee model. ***Government Information Quarterly***, 23(2): 236–248.

Anderson, J. C., Narus, J. A., & van Rossum, W. 2006. Customer value propositions in business markets. ***Harvard Business Review***, 84(3): 90–99.

Babbie, E. 2007. ***The practice of social research*** (11th ed.). Belmonth, MA: Wadsworth/Thomson.

Bailetti, T. 2009. How Open Source Strengthens Business Models | TIM Review. ***Technology Innovation Management Review***. http://timreview.ca/article/226.

Becker, J., Knackstedt, R., & Pöppelbuß, J. 2009. Developing Maturity Models for IT Management: A Procedure Model and its Application. ***Business & Information Systems Engineering***, 1(3): 213–222.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. 2010. Catastrophic cascade of failures in interdependent networks. ***Nature***, 464(7291): 1025–1028.

Chapin, D. A., & Akridge, S. 2005. How can security be measured. ***Information Systems Control Journal***, 2: 43–47.

Christensen, C. M. 2006. The ongoing process of building a theory of disruption. ***Journal of Product Innovation Management***, 23(1): 39–55.

Cresswell, J. 2014. ***Research Design Qualitative, Quantitative, and Mixed Methods Approaches*** (Fourth Edition). Los Angeles: Sage.

Debreceny, R. S. 2006. Re-engineering IT internal controls: applying capability maturity models to the evaluation of IT controls. ***System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on***, 8: 196c–196c. IEEE.

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

Foddy, W. 1993. ***Constructing Questions for Interviews and Questionnaires***. Cambridge University Press, http://dx.doi.org/10.1017/CBO9780511518201.

Fowler, F. J. 2009. ***Survey research methods*** (4th. ed.). Thousand Oaks, CA: SAGE Publications, Inc.

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

Greenhalgh, T., Robert, G., Macfarlane, F., Bate, P., & Kyriakidou, O. 2004. Diffusion of Innovations in Service Organizations: Systematic Review and Recommendations. ***Milbank Quarterly***, 82(4): 581–629.

Gregory, H. 2014, February 23. ***White House Releases NIST Cybersecurity Framework — The Harvard Law School Forum on Corporate Governance and Financial Regulation***. http://blogs.law.harvard.edu/corpgov/2014/02/23/white-house-releases-nist-cybersecurity-framework/.

Gustafson, D. H., Sainfort, F., Eichler, M., Adams, L., Bisognano, M., et al. 2003. Developing and testing a model to predict outcomes of organizational change. ***Health Services Research***, 38(2): 751–776.

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

Lahrmann, G., Marx, F., Mettler, T., Winter, R., & Wortmann, F. 2011. Inductive design of maturity models: applying the Rasch algorithm for design science research. ***Service-Oriented Perspectives in Design Science Research***: 176–191. Springer.

Mellado, D., Blanco, C., Sánchez, L. E., & Fernández-Medina, E. 2010. A systematic review of security requirements engineering. ***Computer Standards & Interfaces***, 32(4): 153–165.

Meneklis, V., & Douligeris, C. 2010. Bridging theory and practice in e-government: A set of guidelines for architectural design. ***Government Information Quarterly***, 27(1): 70–81.

Merabti, M., Kennedy, M., & Hurst, W. 2011. Critical infrastructure protection: A 21st century challenge. ***Communications and Information Technology (ICCIT), 2011 International Conference on***, 1–6.

Meyer, A. D., & Goes, J. B. 1988. Organizational assimilation of innovations: A multilevel contextual analysis. ***Academy of Management Journal***, 31(4): 897–923.

Miron, W., & Hudson, D. 2014. Enabling Employee Entrepreneurship in Large Technology Firms. ***Technology Innovation Management Review***, 4. http://timreview.ca/article/766.

Miron, W., & Muita, K. n.d. ***Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure***. http://timreview.ca/sites/default/files/article_PDF/MironMuita_TIMReview_October2014.pdf, November 4, 2014.

Muegge, S. 2012. Business Model Discovery by Technology Entrepreneurs. ***Technology Innovation Management Review***, (April 2012: Technology Entrepreneurship). http://timreview.ca/article/545.

Murray, A. T., & Grubesic, T. H. 2012. Critical infrastructure protection: The vulnerability conundrum. ***Telematics and Informatics***, 29(1): 56–65.

New York State Senate. n.d. ***Bill S3405-2015***. http://open.nysenate.gov/legislation/bill/S3405-2015, April 5, 2015.

Nili, Y. 2014, August 25. ***Understanding and Implementing the NIST Cybersecurity Framework — The Harvard Law School Forum on Corporate Governance and Financial Regulation***. http://blogs.law.harvard.edu/corpgov/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/.

Peres, R., Muller, E., & Mahajan, V. 2010. Innovation diffusion and new product growth models: A critical review and research directions. ***International Journal of Research in Marketing***, 27(2): 91–106.

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., Mart?, 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.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. ***IEEE Control Systems Magazine***, December 2001: 11 – 25.

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

Rogers, E., & Bhowmik, D. 1970. Homophily-Heterphily: Relational concepts for communication research. ***Public Opinion Quarterly***, 34(4): 523–538.

Rostila, M. 2010. Birds of a feather flock together - and fall ill? Migrant homophily and health in Sweden: Migrant homophily and health in Sweden. ***Sociology of Health & Illness***, 32(3): 382–399.

Singh, A. N., Gupta, M. P., & Ojha, A. 2014. Identifying critical infrastructure sectors and their dependencies: An Indian scenario. ***International Journal of Critical Infrastructure Protection***, 7(2): 71–85.

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.

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

Vespignani, A. 2010. Complex networks: The fragility of interdependency. ***Nature***, 464(7291): 984–985.

Von Wangenheim, C. G., Hauck, J. C. R., Salviano, C. F., & von Wangenheim, A. 2010. Systematic literature review of software process capability/maturity models. ***Proceedings of International Conference on Software Process Improvement and Capabity dEtermination (SPICE), Pisa, Italy***. http://www.inf.ufsc.br/~gresse/download/SPICE2010_Systematic_Literature_vf.pdf.

Wejnert, B. 2002. Integrating Models of Diffusion of Innovations: A Conceptual Framework. ***Annual Review of Sociology***, 28(1): 297–326.

Wendler, R. 2012. The maturity of maturity model research: A systematic mapping study. ***Information and Software Technology***, 54(12): 1317–1339.

Xiao-Juan, L., & Li-Zhen, H. 2010. Vulnerability and interdependency of critical infrastructure: A review. ***Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA), 2010 Third International Conference on***, 1–5. IEEE.

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.

Appendix A – Survey instrument version 1

Adoption of Cybersecurity Capability Maturity Models in Municipal Government Critical Infrastructure Protection

This study aims to quantitatively investigate the impact of a cybersecurity capability maturity model (CMM) based on ISO/IEC 27001 and CMMI and which is tailored to address the unique situation of a municipal government operator of multiple, interdependent critical infrastructures on cybersecurity readiness assessment.

Funding Source: Carleton University, Public Works and Government Services Canada

Date of ethics clearance: January 8, 2015

Ethics Clearance for the Collection of Data Expires: May 31, 2015

This is a study on the Adoption of Cybersecurity Capability Maturity Models in Municipal Government Critical Infrastructure Protection. This study aims to investigate the impact that a cybersecurity capability maturity model has on improving cybersecurity readiness on cyber interdependent critical infrastructures. **The researcher for this study is Walter Miron in the Technology Innovation Management program at Carleton University.**

He is working under the supervision of Prof. Bailetti in the Department of Systems and Computer Engineering.

This study involves one 30 minute survey that will take place online.

While this survey does involve some professional and emotional risks, you have the right to refuse to answer any of the questions. Care will be taken to protect your identity by keeping all responses anonymous.

You have the right to end your participation in the survey at any time, for any reason, up until you hit the the "submit" button. You can withdraw by exiting the survey at any time before completing it using the "Exit and Clear Survey" button located at the bottom of the survey form. If you withdraw from the study, all information you provided will be immediately destroyed. (As the survey responses are anonymous, it is not possible to withdraw after the survey is submitted.)

All research data, will be encrypted and password-protected. The company running the online survey is hostedincanadasurveys.ca based in Canada. The survey company will keep a copy of the survey responses on its servers in Canada. This data will also be encrypted and will be deleted once the survey is complete. Research data will be accessible by the researcher, the research supervisor and the survey company. No names or IP addresses will be linked to any of the data provided.

Once the project is completed, all research data will be kept for five years and potentially used for other research projects on this same topic. At the end of five years, all research data will be deleted.

If you would like a copy of the finished research project, you are invited to contact the researcher to request an electronic copy which will be provided to you as long as the safety of all participants will not be comprised by doing so.

This project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. Should you have questions or concerns related to your involvement in this research, please contact:

REB contact information:

Professor Andy Adler, Chair

Professor Louise Heslop, Vice-Chair

Research Ethics Board

Carleton University

1325 Dunton Tower

1125 Colonel By Drive

Researcher contact information:

Walter Miron

Technology Innovation Management

Carleton University

Tel: 613-520-2600 ext. 8398

Email: walter.miron@carleton.ca

Supervisor contact information:

Dr. Tony Bailetti

Systems and Computer Engineering

Carleton University

Tel: 613-520-2600 ext. 8398

Email: bailetti@sce.carleton.ca

By clicking "submit", you consent to participate in the research study as described above.

There are 17 questions in this survey

Tell us about yourself

This section gathers information for cluster analysis of the study results to determine if municipal size affects views on cybersecurity capability maturity model adoption.

1 []

How many people reside in the municipality that you represent?

Only answer this question if the following conditions are met: 3

Please choose **only one** of the following:

- ○ Fewer than 10,000 residents
- ○ 10,000 to 500,000 residents
- ○ More than 500,000 residents

2 []What is your current role in your organization?

Please choose **all** that apply:

- ☐ CIO / CTO / CSO
- ☐ IT Man-agement
- ☐ Subject Matter Expert
- ☐ Other:

3 []How many years have you worked in IT security?

Please choose **only one** of the following:

- ○ Less than 1 year
- ○ 1 to 5 years
- ○ 5 to 10 years
- ○ 10 to 15 years
- ○ Greater than 15 years

4 []Choose the infrastructures that your municipality operates

Please choose **all** that apply:

- ☐ Electricity
- ☐ Water
- ☐ Transportation Control
- ☐ Emergency Services ☐ Telecommunications
- ☐ eGov- ernment systems / Constituent data
- ☐ Other: _____

Cybersecurity Capability Maturity models

5 []

ISO 27000 includes controls applicable to my needs?

Please choose the appropriate response for each item:

Strongly Disagree	Disagree	Agree	Strongly Agree	Don't Know
○	○	○	○	○

6 []

CMMI includes processes applicable to my needs?

Please choose the appropriate response for each item:

Strongly Disagree	Disagree	Agree	Strongly Agree	Don't Know
○	○	○	○	○

7 []

I currently use a CMM to assess cybersecurity maturity?

Please choose **only one** of the following:

○ Yes

○ No

Impact of cybersecurity capability maturity model

This section explores the impacts of a cybersecurity capability maturity model on cybersecurity readiness assessment

8 []

Regular assessment of cybersecurity readiness maturity is important to the effective operation of my organization.

Please choose the appropriate response for each item:

Strongly Disagree	Disagree	Agree	Strongly Agree
○	○	○	○

9 []

The ability to trial a CMM prior to adoption will ease its introduction in my organization

Please choose the appropriate response for each item:

Strongly Disagree	Disagree	Agree	Strongly Agree
○	○	○	○

10 []

Trialing a CMM prior to adoption would reduce implementation time by;

Please choose the appropriate response for each item:

No change	3 Months	6 months	9 months	12 months
○	○	○	○	○

11 []

How frequently do you re-assess your cybersecurit

Please choose the appropriate response for each item: **readiness?**

Never	every 3 months	every 6 months	every 12 months	More than every 12 months
○	○	○	○	○

12 []

A cybersecurity CMM for interdependent CI would improve our regular security maturity assessment by:

Please choose the appropriate response for each item:

No change	3 Months	6 months	9 months	12 months
○	○	○	○	○

13 []

The compatibility of the CMM with my current environment would improve adoption by:

Please choose the appropriate response for each item:

No change	3 Months	6 months	9 months	12 months
○	○	○	○	○

14 []

Ease of use of a CMM reduces its adoption time by?

Please choose the appropriate response for each item:

No change	3 Months	6 mor	9 months	12 months
○	○	○	○	○

Implementation

15 []

Would a confidential index plotting your maturity level relative to the industry aid in promoting cybersecurity readiness?

Please choose the appropriate response for each item:

Strongly Disagree	Disagree	Agree	Strongly Agree	D
○	○	○	○	

16 []

Practitioners certified in implementing a cybersecurity capability maturity model would aid choosing a partner?

Please choose the appropriate response for each item:

Strongly Disagree	Disagree	Agree	Strongly Agree	D
○	○	○	○	

17 []

Are there any other points that you would like to offer for consideration?

Please write your answer here:

Thank you for your participation in this study.

As a token of appreciation, I will be providing you with links to publications resulting from the research. If you would like to receive a copy of the research results, or have any questions, please contact me at walter.miron@carleton.ca.

Walter Miron

Submit your survey.
Thank you for completing this survey.

Appendix B – Survey instrument version 2

Adoption of Cybersecurity Capability Maturity Models in Municipal Government Critical Infrastructure Protection

This study aims to quantitatively investigate the impact of a cybersecurity capability maturity model (CMM) based on ISO/IEC 27001 and SEI CMMI and which is tailored to address the unique situation of a municipal government operator of multiple, cyber-interdependent critical infrastructures on cybersecurity readiness assessment.

This is a study on the Adoption of Cybersecurity Capability Maturity Models in Municipal Government Critical Infrastructure Protection. This study aims to investigate the impact that a cybersecurity capability maturity model has on improving cybersecurity readiness on cyber-interdependent critical infrastructures. **The researcher for this study is Walter Miron in the Technology Innovation Management program at Carleton University.** He is working under the supervision of Prof. Bailetti in the Department of Systems and Computer Engineering. An overview of the project goals and model can be found here for reference.

This survey has 18 questions and takes less than 5 minutes to complete.

You have the right to end your participation in the survey at any time, for any reason, up until you hit the the "submit" button. If you withdraw from the study, all information you provided will be immediately destroyed.

Care will be taken to protect your identity by keeping all responses anonymous. No names or IP addresses will be linked to any of the data provided. All research data, will be encrypted and password-protected. The survey company will keep a copy of the survey responses on its servers in Canada. This data will also be encrypted and will be deleted once the survey is complete. Research data will be accessible by the researcher, the research supervisor and the survey company. Once the project is completed, all research data will be kept for five years and potentially used for other research projects on this same topic. At the end of five years, all research data will be deleted.

This project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research.

By clicking "submit", you consent to participate in the research study as described above.

There are 18 questions in this survey

Tell us about yourself

This section gathers information for cluster analysis of the study results to determine if municipal size affects views on cybersecurity capability maturity model adoption.

1

How many people reside in the municipality that you represent?

Please choose **only one** of the following:

- ○ Fewer than 10,000 residents
- ○ 10,000 to 500,000 residents
- ○ More than 500,000 residents

2 What is your current role?

Please choose **all** that apply:

- ☐ CIO / CTO / CSO
- ☐ IT Management
- ☐ Cybersecurity Expert
- ☐ Other:

3 How many years have you worked in cybersecurity?

Please choose **only one** of the following:

- ○ Less that 1 year
- ○ 1 to 5 years
- ○ 5 to 10 years
- ○ 10 to 15 years
- ○ Greater than 15 years

4

Public Safety Canada defines ten critical infrastructure sectors. Choose the infrastructures below that your municipality operates

Please choose **all** that apply:

- ☐ Electricity
- ☐ Water
- ☐ Transportation Control
- ☐ Emergency Services / Safety
- ☐ Information and Communications Technology (Telecommunications)
- ☐ eGovernment systems / Constituent data
- ☐ Other:

Cybersecurity Capability Maturity Models

5 Are you knowledgeable with respect to ISO/IEC 27000?

Please choose **only one** of the following:

- ○ Yes
- ○ No

6 Are you knowledgeable with respect to Capability Maturity Modeling such as SEI CMMI?

Please choose **only one** of the following:

- ○ Yes
- ○ No

7 ISO/IEC 27000 is a useful model for ırity ss? cybersec eadine

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Agree	Strongly Agree	Don't Know
Answer	○	○	○	○	○

8 SEI CMMI is useful for assessing cy- maturity? bersecurity

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Agree	Strongly Agree	Don't Know
Answer	○	○	○	○	○

9 Which Capability Maturity Model do you currently use to assess cybersecurity maturity?

Please choose **all** that apply:

- ☐ CMMI
- ☐ SSE-CMM
- ☐ C2M2
- ☐ ES-C2M2
- ☐ ONG-C2M2
- ☐ I do not use a CMM
- ☐ Other: _____

10 Regular assessment of cybersecurity readiness maturity is important to the effective operation of my organization.

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Agree	Strongly Agree
Answer	○	○	○	○

11 How frequently do you re-assess your cyber ecurity readiness?

Please choose the appropriate response for each item:

	Never	Every 3 months or less	Every 6 months	Every 12 months	More than every 12 months
Answer	○	○	○	○	○

Impact of Cybersecurity Capability Maturity Models

This section explores the impacts of a cybersecurity capability maturity model on cybersecurity readiness assessment

12

The ability to trial a cybersecurity Capability Maturity Model prior to formally adopting it would ease its introduction into my organization.

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Agree	Strongly Agree	D
Answer	○	○	○	○	

13

Based on your experience, trialing a cybersecurity Capabilty Maturity Model prior to formally adopting it would reduce implementation time by;

Please choose the appropriate response for each item:

	No change	6 months	9 months	12 months	Don't know
Answer	○	○	○	○	○

14

The compatibility of the CMM with my current environment would improve adoption by:

Please choose the appropriate response for each item:

	No change	6 months	9 months	12 months	Don't know
Answer	○	○	○	○	○

15

A cybersecurity CMM for interdependent Critical Infrastructure would allow us to complete our regular security maturity assessment in:

Please choose the appropriate response for each item:

	No change	6 months or less	9 months	12 months	D
Answer	○	○	○	○	

16

The ease of use of a CMM, in terms of implementation and analysis, reduces it's adoption time.

Please choose the appropriate response for each item:

	Strongly Disagree	Disagree	Agree	Strongly Agree	D
Answer	○	○	○	○	

Implementation

17

Would a confidential index plotting your maturity level relative to peer organizations aid in promoting cybersecurity readiness?

If so, how and to what extent would it aid in promoting cybersecurity?

Please choose **only one** of the following:

- ○ Yes
- ○ No
- ○ Don't Know

Make a comment on your choice here:

18

Are there any other points that you would like to offer for consideration?

Please write your answer here:

Carleton UNIVERSITY
Canada's Capital University

Thank you for your participation in this study. As a token of appreciation, I will be offering you links to publications resulting from this research.

We will be hosting a workshop to further explain the proposed cybersecurity capability maturity model (based on ISO/IEC 27000 and SEI, and tailored to operators of multiple cyber-interdependent critical infrastructures) and benefits. If you are interested in participating please contact me at the email address below.

If you would like a copy of the finished research project, you are invited to contact the researcher to request an electronic copy which will be provided to you as long as the safety of all participants will not be comprised by doing so. Please contact me at walter.miron@carleton.ca if you have any questions relating to the research or survey.

Kindest Regards,

Walter Miron

Date of ethics clearance: January 8, 2015
Ethics Clearance for the Collection of Data Expires: May 31, 2015

This project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. Should you have questions or concerns related to your involvement in this research, please contact:

REB contact information:

Professor Andy Adler, Chair Professor Louise Heslop, Vice-Chair Research
Ethics Board Carleton University
1325 Dunton Tower
1125 Colonel By Drive
Ottawa, ON K1S 5B6
Tel: 613-520-2517 ethics@carleton.ca

Researcher contact information:

Walter Miron

Technology Innovation Management

Carleton University

Tel: 613-520-2600 ext. 8398

Email: walter.miron@carleton.ca

Supervisor contact information:

Dr. Tony Bailetti

Systems and Computer Engineering Carleton University

Tel: 613-520-2600 ext. 8398

Email: bailetti@sce.carleton.ca

Submit your survey.
Thank you for completing this survey.

Carleton UNIVERSITY
Canada's Capital University

Appendix C - Interview instrument

Question	Measure				
How many people reside in the municipality that you represent?	< 10,000		10,000 to 500,000		> 500,000
What is your current Role?	CIO/CTO/CSO	IT Management		Cybersecurity expert	Other
How many years have you worked in Cybersecurity?	< 1 year	1 to 5 years	5 to 10 years	10 to 15 years	> 15 years
Public Safety Canada defines ten critical infrastructure sectors. Choose the infrastructures below that your municipality operates.	Electricity, Water, Transportation control, Emergency Services / Safety, Information and Communications Technology (Telecommunications), eGov / Constituent data, other				
How often do you discuss the impact of interdependent ICT CI on cybersecurity readiness with your peer group?	Never	Seldom	Often	Very Often	Other (explain)
How often do you discuss the difficulty of securing interdependent ICT CI resources?	Never	Seldom	Often	Very Often	Other (explain)
Regulatory awareness on municipal critical ICT infrastructure cybersecurity readiness is:	very low	low	medium	high	very high
Discuss the Model					

Question	Response

ISO/IEC 27000 is a useful model for cybersecurity readiness?	**Strongly disagree**	**Disagree**	**Agree**	**Strongly Agree**	**Don't know**
SEI CMMI is useful for assessing cybersecurity maturity?	**Strongly disagree**	**Disagree**	**Agree**	**Strongly Agree**	**Don't know**
Which Capability Maturity Model do you currently use to assess cybersecurity maturity?	**CMMI, SSE-CMM, C2M2, ES-C2M2, ONG-C2M2, I do not use a CMM, other**				
The ability to trial a cybersecurity capability maturity model prior to formally adopting it would ease its introduction into my organization.	**Strongly disagree**	**Disagree**	**Agree**	**Strongly Agree**	**Don't know**
What is required to conduct a trial of a cybersecurity CMM in your organization?	**Response**				
With respect to security, what level of maturity is your organization operating at?	**very low**	**low**	**medium**	**high**	**very high**
A cybersecurity CMM for interdependent CI will aid in reducing the time to secure ICT resources?	**Strongly disagree**	**Disagree**	**Agree**	**Strongly Agree**	**Don't know**
To what extent does the compatibility of the CMM with your current practices impact adoption?	**Never**	**Seldom**	**Often**	**Very Often**	**Other (explain)**
Ease of use of a CMM is an important factor in it's adoption?	**Strongly disagree**	**Disagree**	**Agree**	**Strongly Agree**	**Don't know**
Are there any other points that you would like to offer for consideration?	**Comments**				

Appendix D – Survey Response Data

Table 17: Survey response data

Variable	Question	Response						
POP	How many people reside in the municipality that you represent?	Fewer than 10,000 residents		10,000 to 500,000 residents		More than 500,000 residents		No Answer
		5		30		3		3
ROL	What is your current role?	CIO / CTO / CSO		IT Management		Cybersecurity Expert		Other
		10		24		2		4
EXP	How many years have you worked in cybersecurity?	Less that 1 year	1 to 5 years	5 to 10 years	10 to 15 years		Greater than 15 years	No Answer
		0	8	8	8		7	10
CIS	Public Safety Canada defines ten critical infrastructure sectors. Choose the infrastructures below that your municipality operates	Electricity	Water	Transportation Control	Emergency Services / Safety	Information and Communications Technology (Telecommunications)	eGovernment systems / Constituent data	Other
		4	24	18	29	25	21	2
		Yes (Y)			No (N)		No answer	
CMM4	Are you knowledeable with respect to ISO/IEC 27000?	10			27		4	
CMM5	Are you knowledgeable with repect to Capability Maturity Modeling such as SEI CMMI?	4			34		3	
		Strongly Disagree	Disagree	Don't Know	Agree	Strongly Agree	No answer	
CMM1	ISO/IEC 27000 is a useful model for cybersecurity readiness?	1	0	15	11	1	13	
CMM2	SEI CMMI is useful for assessing cybersecurity maturity?	1	0	19	5	0	16	
OBSV5	Regular assessment of cybersecurity readiness maturity is important to the effective operation of my organization.	0	1	4	19	12	5	
Trial1	The ability to trial a cybersecurity Capabilty Maturity Model prior to formally adopting it would ease its introduction into my organization.	0	2	5	20	8	6	
Simp3	The ease of use of a CMM, in terms of implementation and analysis, reduces it's adoption time.	0	0	14	9	9	9	
CMM3	Which Capability Maturity Model do you currently use to assess cybersecurity maturity?	CMMI	SSE-CMM	C2M2	ES-C2M2	ONG-C2M2	I do not use a CMM	ISO/IEC 27001
		0	0	0	0	0	38	1
RA3	How frequently do you re-assess your cybersecurity readiness?	Never	Every 3 months or	Every 6 months	Every 12 months	More than every 12 months	No answer	
		3	2	3	15	7	11	
		No change	6 months	9 months	12 months	Don't know	No answer	
Trial3	Based on your experience, trialing a cybersecurity Capabilty Maturity Model prior to formally adopting it would reduce implementation time by;	0	2	1	1	27	10	
Comp3	The compatibility of the CMM with my current environment would improve adoption by:	1	2	1	2	25	10	
RA4	A cybersecurity CMM for interdependent Critical Infrastructure would allow us to complete our regular security maturity assessment in:	0	4	0	4	22	11	
Obsv4	Would a confidential index plotting your maturity level relative to peer organizations aid in promoting cybersecurity readiness?	Yes (A1)		No (A2)		Don't Know (A3)	No answer	
		22		3		12	5	

Table 18: Survey response verbatim

ID	Response **If so, how and to what extent would the index aid in promoting cybersecurity?**
13	provides a benchmark against other organizations and this can be a valuable tool in securing funding
24	Benchmarking relative to others.
37	Would help provide justification for funding.
67	Every municipality used comparator municipalities usually based on population size. If you are shown be far behind what your comparators are doing, it always helps you move

forward on the project.

70 We would be able to show senior management how we stand, and if we are lower than we would like, we may be able to get additional resources.

75 Senior management is always interested in how we compare to our industry partners as it relates to cyber security.

Other feedback

25 Your assumption is that each municipal organization is doing this independently. Not the case. We need a coordinated approach through an org like MISA-ASIM Canada... :)

67 In many cases, though we would like to trial a product, due to purchasing by laws we are unable. We cannot trial something that we will be doing an RFP for as that is seen as an unfair advantage to the trial company.

10 Not sure I buy your primary premise that tracking your maturity better prepares you for a security event. If you think of a different issue such as tracking your earthquake maturity. Do you feel that your response in an earthquake scenario will be better simply because you track your maturity level? I agree that more awareness and education in cybersecurity is useful, but not sure the maturity level buys you much beyond what awareness and education can buy you. Would be curious to see if you have any supporting data showing that organizations have responded better, or more quickly, or recovered faster simply because they have used a Maturity Model.

74 Cybersecurity awareness amongst our CI staff is very low to non-existent

75 Senior management is always interested in how we compare to our industry partners as it relates to cyber security.