The cybersecurity governance in changing the security psychology and security posture: insights into e-procurement

Anisha Banu Dawood Gani

Logistics and Supply Chain Management Research Cluster,
Faculty of Industrial Management,
Universiti Malaysia Pahang,
26300, Malaysia
Email: anisharaffid@gmail.com

Yudi Fernando*

Logistics and Supply Chain Management Research Cluster,
Faculty of Industrial Management,
Universiti Malaysia Pahang,
26300, Malaysia
Email: yudi@ump.edu.my
and
Management Department,
BINUS Online Learning,
Bina Nusantara University,
11530, Indonesia
Email: yudi.fernando@binus.ac.id
*Corresponding author

Abstract: Security is a consistent and growing concern for e-commerce and e-procurement solutions which demand for secure transactions to ensure the confidentiality, integrity and availability of data. E-procurement is vulnerable to cyberattacks resulting in increasing demand for cybersecurity governance. Cybersecurity governance is needed to manage the cyberattacks and ensure the important assets of the company is well protected. The aim of this study is to identify the practices for an effective cybersecurity governance by examining and synthesising existing cybersecurity and cybersecurity governance maturity models and framework from the literature and industry. This study has selected and compared prominent cybersecurity maturity models such as cybersecurity governance maturity model (CSGMM) and cyber preparedness (cyber prep) framework by adapting the taxonomy of software improvement environments method. From the synthesis, 12 practical measures were identified and recommended to manufacturing firms for an effective cybersecurity governance.

Keywords: cybersecurity; e-procurement; cybersecurity governance; cybersecurity maturity models; cyber preparedness; cyber prep; cybersecurity governance maturity model; CSGMM; maturity models.

Reference to this paper should be made as follows: Gani, A.B.D. and Fernando, Y. (2021) 'The cybersecurity governance in changing the security psychology and security posture: insights into e-procurement', *Int. J. Procurement Management*, Vol. 14, No. 3, pp.308–327.

Biographical notes: Anisha Banu Dawood Gani is a PhD candidate and has research interests in the areas of cyber supply chain security, green and energy efficiency in the logistics and supply chain management research cluster at the Faculty of Industrial Management, Universiti Malaysia Pahang. She received her MBA in Service, Science, Management and Engineering (SSME) from Graduate School of Business Universiti Sains Malaysia in 2004. She has over 20 years of experience in manufacturing industry with product lifecycle management and supply chain as her areas of expertise. Professionally, she holds an operations manager role managing several divisions and teams, providing key support in product life cycle and marketing areas. She is also a certified 6-Sigma Green Belter.

Yudi Fernando holds a PhD degree and is the Editor-in-Chief of *International Journal of Industrial Management* and the Managing Editor of *Journal of Governance and Integrity* at the Faculty of Industrial Management, Universiti Malaysia Pahang. He is an Honorary Lecturer at the Binus Online Learning. He has been working in the electronics industry for several years. His current research interests are green operations management, service management, logistics and sustainable issues in supply chain management. He is a Research Committee Chair and founding member of the Malaysian Association of Business and Management Scholars (MABMS) formerly known as an Academy of Business and Management (ABM). He is also a member of the Society of Logisticians, Malaysia/Pertubuhan Pakar Logistik Malaysia (LogM). He serves as a technical committee in international conferences and invited speaker in various universities.

1 Introduction

Manufacturing firms are facing radical changes because of the global interconnectivity, digital data exchange frequencies and the need for real-time information. The past decade has seen tremendous growth in the global use of IT as a decisive factor that significantly contributes to competitive advantage (Tooranloo et al., 2018). One organisational function and supply chain activity which plays a significant role in this digital age is the field of procurement. E-procurement has gained attention with the rapid rise of business transactions over the internet. However, while the research in the area of integration with e-procurement systems have risen, studies are showing there is little attention given for security aspect of this integration that responds to the need for accurate and secure information exchange; which has become essential to doing business (e.g., Stephens and Valverde, 2013). Security is a consistent and growing problem for e-commerce and procurement solutions. Secure transactions are essential if organisations are to fully realise the benefits of e-procurement which include increased productivity, lower purchasing pricing, streamlined processes, reduced order fulfilment time and greater budgetary control; all of which can contribute to increasing the firm's competitive advantage. In order to drive cybersecure culture in a manufacturing firm, the security psychology must be changed from the inside out, and for that, cybersecurity should not

be treated as a technical issue but rather viewed as a business issue. Top management play a pivotal role in setting the security culture tone within a firm and drive policies to improve its security posture. The cybersecure culture can lead to supplier integrity and compliance on cybersecurity standards. Fernando et al. (2019) postulated that risk uncertainty can be reduced in quality of materials if the firm has better supplier integrity.

Cybersecurity in the digital age is very important and an integral part of information technology (Wiryawan et al., 2019). Inherently, the security and privacy of procurement transactions is a major concern for most organisations especially where payment details and other pieces of sensitive information are sent over the internet. Cyberattackers often target the weakest link of the supply chain and penetrate through supplier's firewall to get access to log-in credentials and retrieve commercially sensitive information's (such as invoice, bid information, purchase order systems, customer information, bank account details, credit card, etc.) (Setty, 2018). According to Rogers and Choi (2018), over 60% attack was reported on US firms in 2017. The attackers were found using IT purchasing/procurement systems which involved access of suppliers and other third parties. If not managed properly, the system integration which has been practiced by the modern manufacturing firms has potential opportunities for cyberattack and insecurity. According to Fernando and Saththasivam (2017), the procurement systems integrated in the supply chain need to be responsible to the community's well-being. The manufacturing systems which tend to give accesses to its data to supplier and other third-party vendors has increased the susceptibility for attack. It is imperative for the manufacturing firms to increase the awareness of industrial control system technologies and utilise standard protocols in order to mitigate the attacks (Knowles et al., 2015). The firm's understanding on the cybersecurity regulation and systems protection are needed to protect the data and business information from cyber-attacks (Srinivas et al., 2019). Rogers and Choi (2018) suggested that a supplier's cybersecurity practices should be treated similarly to its quality performance. Effective communication among supply chain networks on data sharing and data security is essential, and guidelines should be written properly to ensure customers data are not abused by unauthorised parties (Fernando et al., 2018).

Cybersecurity governance therefore is needed to manage the cyberattacks and ensure the important assets of the company is well protected. Manufacturing firms need to put cybersecurity at the very heart of the business to address increasing data threats; especially after being ranked as the most targeted industry for cyberattacks (IBM, 2018). Having a standard dashboard on metrics, resources, and compliance as a measure-of-success is no longer enough. Manufacturing firms must now drive and implement effective methods to identify and protect the triad rules of its information assets'; confidentiality, integrity and availability (CIA). However, according to Boyson (2014) purely technical approaches to cybersecurity will not suffice. Security is a business issue and not merely technical (Dutta and McCrohan, 2002). This means, it is unrealistic to apply all possible security controls to every threat, due to budget and time pressures, feasibility and other organisational priorities, rendering researchers taking a longer list of possible mitigations and down-selecting to a shorter list based on some defined criteria or goals (Llansó et al., 2019).

As firms become more reliant on technology, the criticality of improving the security culture in the firm and transforming the security psychology into actual security conscious behaviours are essential for a secure supply chain. Three fundamental domains of an effective cybersecurity strategy are people, processes and technology (Abawajy,

2014). Ultimately the board of directors (BOD) and top management are accountable to drive the direction for how a firm's security is perceived, prioritised, managed, and implemented. In the academic field, cybersecurity governance is relatively new research concept thus publications in this area is rather sparse. Despite the recognition that cybersecurity governance plays an important role in ensuring cybersecurity, scholars are still highly debating and researching the efficacy of cybersecurity governance implementation (De Bruin and Von Solms, 2016a). Nevertheless, there has been several maturity models developed to enhance cybersecurity. In general, cybersecurity maturity models (CMM) are commonly used as an instrument to conceptualise and measure maturity of a firm or a process regarding some specific target state (Schumacher et al., 2016). CMM provide, to some extent, a roadmap for firms for measuring, assessing, and enhancing cybersecurity (Le and Hoang, 2017).

However, capability maturity models like CMM are criticised for multitude of almost identical maturity models and a non-reflective adoption of the maturity model blueprint (Becker et al., 2009; Pöppelbuß and Röglinger, 2011). Moreover, information and awareness are lacking about the most suited model to be applied for a given situation (Miron and Muita, 2014). Additionally, there are cases where maturity models do not provide easily interpretable information for the executives and operations managers (De Bruin and Von Solms, 2016b). This aggravates the confusions already being faced by the firm's management who do not fully understand how the firm can be at risk and what action should be taken to mitigate it (Aradea et al., 2019).Therefore, the aim of this study is to identify the practices for an effective cybersecurity governance by examining, comparing and synthesising existing cybersecurity and governance maturity models and framework from the literature and industry. Following which, this study conceptualises recommendation on proactive practices to mitigate cyber risks in the manufacturing industry.

The remainder of this paper is conceptualisation of the topic by reviewing literatures on the capability maturity models and the rationale for maturity models selection in this study, followed by cybersecurity governance. Next, methodology is presented and subsequently followed by the results of the analysis. Finally, a discussion on the synthesis is presented before concluding. Research limitations and future research opportunity are mentioned for scholars to consider.

2 Capability maturity model and rationale for selection

Capability maturity models was originally developed by the Software Engineering Institute (SEI) in the mid-1980 and represents a path of improvements recommended for organisations that want to increase their software process capability (Wendler, 2012). Similar definition has been adapted in different fields including cybersecurity. A cybersecurity capability maturity model (C2M2) provides a benchmark by which an organisation can assess the current level of maturity of its practices, processes, and set goals and priorities for improvement in cybersecurity (Rea-Guaman et al., 2017). The C2M2s are usually depicted through the lenses of

1 dimensions or common concepts of organisation processes

2 indicators for the objectives that must be fulfilled

3 levels of maturity from initial to advanced.

On the one hand, there are numerous C2M2s used in scientific articles, however the commonly used models according to a systematic study done are identified as systems security engineering capability maturity model (SSE-CMM), C2M2, community cybersecurity maturity model (CCSMM) and national initiative for cybersecurity education (NICE) – capability maturity model (Rea-Guaman et al., 2017). However, a study by De Bruin and Von Solms (2016a) have noted the isolated nature of these maturity models which does not enable a firm to assess its cybersecurity governance maturity. Thus, factoring in the existing maturity models to develop a comprehensive cybersecurity governance maturity model, cybersecurity governance maturity model (CSGMM) was introduced by incorporating most of the existing maturity models as its sub-models.

CSGMM framework is modelled from 15 established standards from reputable universities and government agencies (De Bruin and Von Solms, 2016a) and is referenced in several studies pertaining information security, cybersecurity and cybersecurity governance (e.g., De Bruin and Von Solms, 2017; Maynard et al., 2018). CSGMM comprises several integral maturity models to determine the overall cybersecurity governance maturity (De Bruin and Von Solms, 2016b). The initial model consisted of five aspects to assess the firm's cybersecurity efforts which are cybersecurity:

1 capability

2 contingency

3 capacity

4 conformance

5 threat.

In 2016, two more components were added to the adapted into the CSGMM model, which were the cybersecurity legal and cybersecurity ethics. As this model covers wide range of organisational aspects applicable to manufacturing industry, it is chosen for this study.

On the other hand, there are cyber preparedness (cyber prep) framework such as the ones developed by MITRE corporation who manages federally funded research and development centres (FFRDCs) supporting US government agencies. There are two cyber prep frameworks by MITRE;

1 cybersecurity governance (2010)

2 cyber prep 2.0 (2017).

MITRE's cyber prep framework was modelled after numerous maturity models and frameworks as well. It merges multiple components of cybersecurity strategies from 18 maturity models/frameworks, including seven from cybersecurity governance and other models. Cyber prep is a popular framework used in studies surrounding cyber prep and assessing cyber threat level (e.g., Perumal et al., 2018; Mattern et al., 2014). Adopting the conventional maturity models, cyber prep methodology emphasises on reducing risks due to cyber dependencies. It is because of this cyber context that distinguishes cybersecurity from conventional information security. In cyber prep, there are five levels to categorise a

firm's preparedness depending the beliefs and view of the threat it faces, the strategies to overcome those threats and the firm's approach to cybersecurity governance (MITRE, 2010). Cyber prep 2.0 increases the knowledge regarding continuous threats (i.e., advance persistent threats) and in doing so raises awareness of the importance of investing in security tools and resources to mitigate those persistent risks. Together, these two frameworks enable the understanding of threat landscape and developing and implementing appropriate mitigations for a manufacturing firm based on the threat it faces.

It is noted that cyber prep is not a capability maturity model (MITRE, 2017), because the level of a firm's capability will continually vary according to the threat and risks it faces, therefore the extent of how it prepares to meet those risks would also vary. Given the different characteristics drive different aspects of preparedness, the two cyber prep frameworks are reviewed in concert to identify recommended practices for effective cybersecurity governance more widely. The three maturity-model and frameworks would be examined to identify the security posture elements (e.g., practices, processes, organisational structure) which could elevate a manufacturing firm's cybersecurity maturity level.

A fourth model which was considered for this study was cybersecurity capability maturity model (CM^2) by Barclay (2014). While not a CSGMM, CM^2 is a CMM that helps firms or a nation to identify their capability and ability to manager cyber-risks (Barclay, 2014). However, upon review, CM^2 turned out to be an infancy stage model (Barclay, 2014), hence the characteristics of the components across each pillar were not found at the point where this study was undertaken. Therefore, comprehensive examination cannot be done on this model to effectively contribute to this study, thus, not considered as among a primary review model of this study.

Table 1 CM^2 optimising maturity level summary

Constituents	*Stages-optimising*
Attitude towards threat and vulnerabilities	Highly proactive
Extent of technological development	Pervasive innovation
Societal response	Pervasive levels of awareness, efficiency and flexibility
Technical measures	Highly structured capability-based measures
Business measures	Highly structured capability-based measures
Legal and regulatory measures	Highly structured capability-based measures
Operational measures	Highly structured capability-based measures
Education/capability building	Highly structured capability-based measures

Source: Adapted from Barclay (2014)

Nevertheless, a high-level overview of the CM^2 capabilities, the 'optimising' maturity level is summarised as being proactively started in all indicators of the models (Barclay, 2014). It is apparent that for developing an effective strategy, a whole-rounded approach which encompasses education, training, legal, technical, operational as well as capacity building is necessary. Similarly, the approach to threat is proactive at this stage. The overview on CM^2's most mature state, i.e., optimising state components, are captured in

Table 1. These components shall be considered when a recommended practice is devised at the end of this paper.

Together, these models and frameworks components provide comprehensive insights into assessing the maturity level of a firm in combating cybercrime. As the focus of this study is examining and outlining recommendation on robust measures to mitigate cyber risk, the validity of these maturity model and frameworks will not be tested, and therefore, out of scope of this paper's objective.

3 Cybersecurity governance

IT governance institute (ITGI) defines governance as a set of responsibilities and practices exercised by those responsible for a firm (e.g., the board and executive management in a firm) with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly (CISA, 2013). US CERT defines cybersecurity governance as directing and controlling an organisation to establish and sustain a culture of security in the organisation's conduct (beliefs, behaviours, capabilities, and actions) treating adequate security as a non-negotiable requirement of being in business. On a similar tone, National Institute of Standards and Technology (NIST) (CISA, 2013) defines information security governance in greater detail; that it is:

1 the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies

2 are aligned with and support business objectives

3 are consistent with applicable laws and regulations through adherence to policies and internal controls

4 provide assignment of responsibility to manage risk.

Ultimately, cybersecurity governance refers to the component of enterprise governance that addresses the enterprise's dependence on cyberspace in the presence of adversaries. It is becoming more and more critical for a manufacturing firm to have a good, strong cybersecurity strategy especially with rising number of cyberattacks and security breaches. However, research reveals there is a lack of a cybersecurity culture because there is a lack of top management leadership to create an effective information security culture to protect the information assets of the business (Scully, 2014). Further, according to Scully (2014), ad hoc approach to managing cyber risk exposes businesses to cyber-attack. Thus, it is not surprising that the importance of top management's role in being committed to achieve firm's objectives, including security, has proven to reinforce the right kind of behaviour among the employees in order to develop a sense of ownership and as a basis of motivation to continue embodying the security culture (Yusliza et al., 2019). The only way to make cybersecurity important is for the firm's leader to make it as part of their firm's DNA.

The absence of a good cybersecurity strategy can cause significant problems for a business. Thus, as the ultimate guardians of customer and other stakeholder data, top management must take a proactive stance and lead a culture of security; by making

cybersecurity considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions. A recent study on information security assessing the importance of managements role found that the trend of considering IT professionals being responsible for information security has changed and now management is believed to be responsible for information security (Soomro et al., 2016). Organisations are advised to adopt a more holistic approach to information security management to include management participation from top level management; human resources management; information security policy development and execution; information security awareness and training; and the involvement of strategic decision makers. Cybersecurity governance, therefore, is fundamental to effective operational preparedness to manage cybersecurity risks.

4 Methods

One of the aims of this study is to compare the different maturity models to identify the proactive measure elements that a firm is recommended to implement, to achieve a maturity stage in their firm's cybersecurity level. Adapting the method that Khoshgoftar and Osman (2009) has used, this study uses a two-step approach; the first is to select some models for comparison. In that regard, this study focuses on recent maturity models on cybersecurity governance and CMMs chosen based on the findings from past systematic reviews. The selected models from cybersecurity governance are;

1 CSGMM

2 cyber prep and cyber prep 2.0.

Meanwhile, a third model named CM^2 will be examined from a cybersecurity maturity perspective.

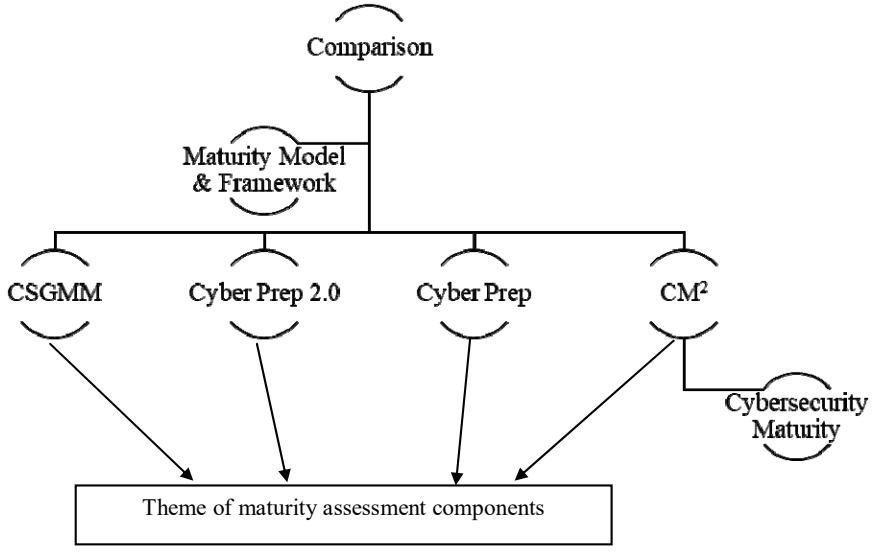
The second step is to find the basis for comparing the maturity model and frameworks with each other. Therefore, the methods to be able to carry out the comparative study of the mentioned models are based on the taxonomy of software improvement environments proposed by Halvorsen and Conradi (2001). This method is also used by several other authors on the topic of maturity model comparison (e.g., García-Mireles et al., 2015; Rea-Guaman et al., 2017). The taxonomy described by Halvorsen and Conradi (2001) provides a list of 25 relevant features for the comparison which are grouped into five categories, namely:

- features that describe the general attributes of the improvement environment
- features that describe how the environment is used
- features that describe how is the relationship between the features related to the attributes of the organisation and the environment in which it is used
- features related to the quality dimension
- features that describe the results of using the environment, the costs of achieving the results, and the methods used for its validation.

In adopting the approach of Rea-Guaman et al. (2017), this taxonomy was adapted to be applied in the comparison of the CM^2 by excluding the quality and result categories as

they did not allow the comparison of the CM² (Rea-Guaman et al., 2017). Moreover, the features of the general, process and organisation categories were redefined. Under general classification, an overview of the selected cybersecurity and CSGMM and frameworks was considered. Next, for process category, each of the maturity models and frameworks highest level maturity level is summarised and finally for the organisational category, the recommended best practices and the recommended owner is then proposed. The process for model comparison is depicted in Figure 1.

Figure 1 The process of maturity model and framework comparison



5 Results

As this study is interested on the measures that elevates the level of maturity in a firm, the highest or the most mature level of the model or framework is selected for qualitative comparison. Table 2 shows the comparison of the models regarding its objectives, constituents and level of maturity stages. This means that for CM², CSGMM, and cyber prep; the optimising stage, 4th level of maturity and pervasive agility maturity elements would be synthesised respectively. In each these stages, maturity assessment components are categorised according to their theme of the constituents. Model CM² has eight constituents and 6 levels of maturity ranging from 0 to 5. CSGMM has seven sub-models as its constituents with maturity stages broken down into three key categories (i.e., people, process, technology) with four levels of maturity rankings. However, the category is not defined for cybersecurity legal maturity model (CSLMM) and cybersecurity ethics maturity model (CSEMM). Cyber prep and cyber prep 2.0 frameworks also has three categories of constituents namely governance, operations and architecture and engineering with five maturity level rankings for each.

Table 2 Selected cybersecurity and CSGMM and frameworks overview

Model	*Author(s)*	*Objective*	*Constituents*	*Stages*
CM^2	Barclay (2014)	Illustrates the stages of readiness or preparedness to respond to threats, vulnerabilities and technological advancement that exists within the continuously evolving environment. The six stages of capabilities focus not on the threats, but the capabilities needed to achieve security advantage.	1 Attitude to threat and vulnerabilities 2 Technological development 3 Societal Response 4 Technical measures 5 Business measures 6 Legal and regulatory measures 7 Operational measures 8 Education/capability building	0 Incomplete 1 Performed 2 Managed 3 Defined 4 Quantitatively managed 5 Optimising
CSGMM	De Bruin and Von Solms (2016b)	To determine the cybersecurity maturity of a firm. CSGMM comprise of several integral maturity models to determine the overall cybersecurity governance maturity	Cybersecurity capability maturity model (CSCMM) Cybersecurity contingency maturity model (CSCtMM) Cybersecurity capacity building maturity model (CSCBMM) Cybersecurity conformance maturity model (CSCfMM) Cybersecurity threat maturity model (CSTMM) Cybersecurity legal maturity model (CSLMM) Cybersecurity ethics maturity model (CSEMM)	Sub-model categorisation into: people, processes, and technology; measurement level 1–4 Sub-category not specified, measurement level 1–4
Cyber prep and cyber prep 2.0	MITRE (2010, 2017)	To provide to assess and identify gap of a firm's cybersecurity governance structures as well as practices.	Governance Operations Architecture and engineering	5 Agility 4 Resilience 3 Awareness 2 Critical information protection 1 Basic

Source: Adapted from Barclay (2014), De Bruin and Von Solms (2016b) and MITRE (2010, 2017)

CSGMM and cyber prep framework was reviewed to examine further the components which has the highest ranking for each constituent and/or its sub-models. The summary of the rankings for each constituent are summarised in Table 3 (for CSGMM) and Table 4 (for cyber prep) respectively.

Table 3 Summary of highest ranked components in CSGMM

Constituents	*Category*	*Level 4*
Cybersecurity capability maturity model	People	The firm has invested in and approved cybersecurity strategies and has periodic reviews to ensure its validity
	Processes	The cybersecurity strategies are constantly updated to keep it relevant
		The firm's strategy includes cybersecurity and processes depicts the alignment with strategy
	Technology	The firm's both hardware and software are relevant, and up-to-date
Cybersecurity contingency maturity model	People	The firm has established a functional team in its critical incident response centre (CIRC)
		The CIRC comprises of specialised taskforces
	Processes	Policies governing and regulating incident response controls exists and regularly reviewed for relevance and adequacy
		CIRC effectiveness is audited regularly to ensure relevance
	Technology	Fully functioning controls that triggers upon threat detection
Cybersecurity capacity building maturity model	People	Specialised team trained on cybersecurity to conduct or coordinate accreditation and trainings
		Involvement of top management in understanding cybersecurity tactical strategies are in-line with corporate strategy
	Processes	Prioritised funding allocation for cybersecurity
	Technology	Cybersecurity controls exists and is accessible to all level of the employees
Cybersecurity conformance maturity model	People	Firm's security culture embodied by all level of employees
	Processes	Adherence to cybersecurity by all functions within the firm well documented
	Technology	Not measured
CSTMM grid	People	Appointed taskforce to assess firm's threat and vulnerability exists
	Processes	The threat and vulnerability assessment policy exist and reviewed and enhanced for relevancy
	Technology	Patch management is automatically rolled-out according to company policies

Source: Adopted from De Bruin and Von Solms (2016b)

Table 4 Summary of highest ranked aspects in cyber prep

Area	*Aspect*	*Pervasive agility*	*Desired approach*
Governance	Governance structure	Intelligently evolving	Proactive management
	Internal integration	Collaboration	Cooperation,
	Mitigation philosophy	Innovation leadership	Risk awareness
	Adaptability	Adaptable alternatives	Established alternatives
	External coordination	Collaboration	Cooperation
Operations	Security posture assessment	Integrated mission situational awareness	Threat-informed scanning and monitoring
	Incident management	Integrated defensive operations	Incident management
	Threat intelligence and analysis	Innovative	Proactive
	Forensic analysis	Innovative	Proactive
	Training and readiness	Integrated readiness	Informed readiness
Architecture and engineering	Architectural definition	Extensive	Data-centric
	Security engineering orientation	Integrated risk	Compliance
	Functionality	Extended cyber resiliency	Moderate cybersecurity
	Versatility	Highly evolvable	Tailorable, subject to firm's capacity

Source: Adopted from MITRE (2017)

6 Discussion

CSGMM had sub-category classifications of people, process and technology; with each of the category has components broken down by each maturity level. The highest maturity level on this model which was examined level 4. In synthesising, several practices are prominent in order to achieve this level of maturity according to this model. They are as follows:

1 cybersecurity should be a part of strategic decision

2 periodic review on cybersecurity strategy with top management must be held (e.g., BOD, senior managers)

3 ability of top management to understand technicalities; or for top management be represented by technical savvy personnel in order to better steer the firm's direction towards cybersecurity culture

4 cybersecurity training and awareness to all employees must be provided to up skill employees in order to execute planned strategy

5 form a dedicated team to champion cyber defence strategy; a specialised focus in imperative to drive the right strategy, focus and mindset

6 conduct periodic compliance audit to assess depth and breadth of coverage

7 system integration security and alert capability in the event of intrusions or anomaly in processes

8 regular, and where possible, automated system patches

9 compliance with international and local with regulations.

Based on these practices to obtain the highest maturity level stated above, a classification of the grouping based on the category and constituents is summarised. The corresponding recommended practices and proposed owner from CSGMM synthesis is then provided in Table 5. The recommended owner is defined based on the influence required for each practice's implementation, whether it is the BOD, SM, OM or IT personnel. For clarity on constituent segregation, the summary is consolidated according to the CSGMM category.

Cyber prep framework is quite comprehensive evaluation list. Its highest preparedness stage is the pervasive agility; which imply the ability of the firm to maintain operations on a continuing basis and adapts to current and future coordinated, successful attacks, regardless of their origins. To achieve this level, the firm required to have a highly agile, adaptive, and flexible structure that permeates all aspects of the organisation (including planning, supply chains, collaboration, architecture, governance, and resources) (MITRE, 2010).

Table 5 Recommended practices and owner from CSGMM synthesis

Category	*Constituents*	*Recommended practice*	*Recommended owner*
People	Capable	Establish cybersecurity strategies that are in line with business strategies	BOD, SM
	Capable	Active involvement in periodic review and update according to business strategy and changes	BOD, SM
	Contingency	Form fully functioning and specialised incident response team	SM
	Capacity	Technical data interpretation for boards review or board be represented by technically savvy member for sound decision making	BOD, SM
	Capacity	Provide professional accreditation, cybersecurity education, training and awareness to all employees and firm	SM, OM
	Conformance	Enforce legal and regulatory compliance requirements throughout all structures of the organisation. Implement audit measures.	BOD, SM, OM
	Threat	Security personnel performs threat and vulnerability scanning according to the organisation's policies	SM, OM

Source: Authors

Table 5 Recommended practices and owner from CSGMM synthesis (continued)

Category	*Constituents*	*Recommended practice*	*Recommended owner*
Process	Capable	Implement process and policies which are aligned with the organisation's cybersecurity strategy	OM
	Contingency	Ensure policies that drive incident response controls exist and are constantly updated and maintained	SM, OM
	Contingency	Form CIRC	BOD, SM
	Contingency	Constantly audit CIRC effectiveness according to qualitative and quantitative controls	SM, OM
	Capacity	Allocate budget for complete cybersecurity education, training and awareness	BOD, SM
	Conformance	The cybersecurity strategy must be identified and communicated as component of critical infrastructure for the firm	BOD, SM
	Threat	Constant review and update to the threat and vulnerability assessment must be made as part of company policy	SM, OM, IT
Technology	Capability	The organisation's cybersecurity controls – both hardware and software – are properly configured and maintained and are constantly reviewed and upgraded as, if and when needed	IT, OM
	Contingency	Ability for incidence response controls automatically raise alerts when suspicious activities have been detected	SM, OM, IT
	Capacity	Cybersecurity education, training and awareness controls do exist and can be used by any staff	SM, OM
	Threat	Patch management is done automatically according to company policies	OM

Common theme as the CSGMM was also noted in cyber prep; namely, making cybersecurity as part of strategic planning with top management championing the effort, training and awareness tailored to employees and systems integration with ability to detect and alert any anomalies found. However, there was an emphasis on collaboration between not only internal stakeholders, but also external stakeholders emphasised in cyber prep which was not explicitly found in CSGMM. This external collaboration marks a mature governance approach, and one that is significant, especially with the trends of attacks in manufacturing industry were possible due to a third-party network vulnerability. Similarly, collaboration with industry peers allow benchmarking possible

and with adequate measures taken; provide assurance to customers that their privacy and product integrity will be safeguarded. The summary of the recommended practices and proposed owner from cyber prep framework synthesis is provided in Table 6.

Table 6 Recommended practices and owner from cyber prep synthesis

Constituents	*Stages*	*Recommended practice(s)*	*Recommended owner*
Governance	Pervasive agility	• Setup governance team that is under the purview of the top management and include members from security personnel's (including physical security, personnel security, business continuity, SCRM, ICT architecture, business process engineering, operations security, and cybersecurity) and strategic planning. • Establish provisions for collaboration with cybersecurity counterparts in other organisations in the organisation's mission or critical infrastructure sector, as well as in peer, partner, supplier, and customer organisations in support of a shared threat/incident awareness preparation and response.	BOD, SM
Operations	Pervasive agility	• Establish cyber situational awareness team who manages the mission of the cybersecurity posture. The team should consist of cyber defenders, tool developers and forensic analysts. • Provide tailored training and awareness material to all employees based on threat intelligence updates. • Cultivate internal and external collaborative culture. Establish contingency plans and joins business continuity plans to minimise mission disruptions.	SM, OM
Architecture and engineering	Pervasive agility	• Security architecture implemented is built-in with alerts and data to track and measure resiliency; ability to detect anomalies and trigger for review.	OM, IT

Source: Authors

To aid manufacturing firms implement robust measures to manage cybersecurity issues effectively, a review on CSGMMs and frameworks has been undertaken. The synthesis on these literatures enabled the following practical guidelines to be conceptualised and provided as a recommendation to manufacturing firms:

1 Top management must be involved and drive the cybersecurity initiatives.

2 Participation from all managerial level and divisions are required to obtain comprehensive mitigation plans and to avoid crucial technical details are not 'lost in translation'.

3 Sufficient budget allocations for the cybersecurity initiatives is needed depending on the maturity level aspired.

4 Regular cybersecurity risk assessment and compliance analyses should be conducted to both internal and external stakeholders, especially third-party vendors.

5 Ensure business partner compliance with cybersecurity policy. Include penalty clause for non-compliance as part of policy.

6 Form dedicated team to exclusively manage, protect and respond to anomalies in the system.

7 Built-in systems with intelligence to alert on any intrusions.

8 Ensure all employees are trained and aware on cyber breach implications. Non-compliance to process and policies should warrant penalty to demonstrate graveness of violation.

9 Segregate sensitive data with publicly available data and control access accordingly.

10 Perform regular, and where possible, automated system patches.

11 Comply with regulations.

12 Regular, periodic review on cybersecurity strategy with top management.

Table 7 Cyber supply chain security practices

Domains	*Instrument items*
Governance	Managing cybersecurity issues
	Cybersecurity plans
	Government/ industry-initiated cybersecurity guidelines
	Verify security guidelines
	Adjusted cyber supply security structure to changing conditions.
Systems integration	Coordinate security plan with major suppliers
	Jointly developed/implemented document retention policy on cyber supply chain risk.
	Provide frequent status updates on current or emerging cyber supply chain risks
	Provide timely information to respond to contamination/security incidents.
Operations	Has processes to prevent a contamination/security event
	Has processes to detect a contamination/security event
	Has processes in place to respond to a contamination/security event
	Security audits
	Audits the security procedures of contract manufacturers
Relational collaboration	A close relationship with our supply chain partners
	Maintain a sustainable relationship
	Share and exchange security information
	Share accurate and timely security information with main partners.
	Carefully selects low risk and high security business main partners.

Source: Authors

Figure 2 An interconnected of cyber supply chain security practices (see online version for colours)

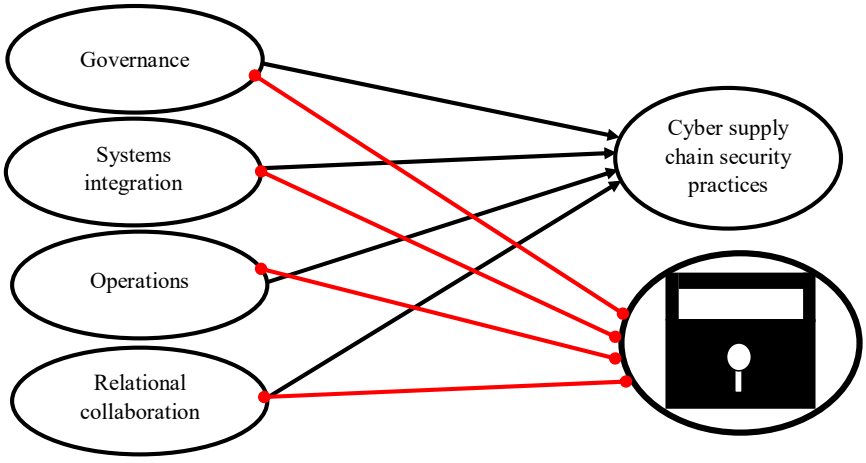


Table 7 and Figure 2 show the instrument items that the firms need to consider practicing the cyber supply chain security. This study defines cyber supply chain security practices as the cyber control mechanism and management control systems on information processing including capture, store, distribute the necessary information among the supply chain networks which involve end to end integration on governance, systems integration, operations and relational collaboration.

7 Conclusions

An effective cybersecurity measures require a combination of people, process and technology to be in place. Rather than reactive approach, manufacturing firms must proactively be prepared to detect, respond and recover from series of possible attacks. According to Fernando and Chukai (2018), risk assessments have been proven to reduce unnecessary operational activities and leads to better operational performance. The review of the current CM^2 highlighted that, although many models exist, none are specifically created to address security intrusions as a result of e-procurement per se. Rather, they are on specific industry sub-sectors and are all at a high level. Even with the extension of the CMM as a CSGMM; in the same way, one of the drawbacks of the CSGMM is that it does not offer explicit recommendation on practices that the firm should adopt to achieve maturity at any given state of being; but rather it assesses the 'as-is' practices of the firm (Pöppelbuß and Röglinger, 2011). As such, the maturity model is applied reactively to derive and prioritise improvement measures.

This study addresses this gap by providing practical recommendations to manufacturing firms to achieve highest level of maturity level in combating cybersecurity issues. That said, security culture and employee psychology must be changed from the inside out, and for that, cybersecurity must be treated as a business issue rather than a technical issue. This shifts the accountability of ensuring cybersecurity be considered as business objective, and adopted as strategic risk, to the top management. Driving the culture of understanding that security problems cannot be solved with technology alone is

a first step towards establishing a mature cyber prep level. Effective cybersecurity measures require a combination of people, process and technology to be in place. Rather than reactive approach, manufacturing firms must proactively be prepared to detect, respond and recover from series of possible attacks.

8 Limitations and future research

While the study has contributed to the literature by providing actionable and practical guidelines in order to increase the security posture of the manufacturing firm, there are limitations to this study. Firstly, this study is conceptualised based on literature reviews, thus empirical studies are needed to assess the extent of security maturity achieved by implementing these recommended guidelines. Next, the scope of the analysis and synthesis of this study is based on existing maturity model which has been found most commonly used by scholars via systematic reviews. There are other maturity models not considered in this study which may enrich the guidelines, thus is recommended for future researchers to consider and expand upon. Finally, the context of this paper is limited to manufacturing firm perspective, thus future research can assess the suitability of the guidelines recommended to other industries. Echoing with the Jasmi and Fernando (2018) finding, this study suggest that a firm should prepare a blueprint for a security programme for long-term business survival.

Acknowledgements

The authors convey their appreciation to the Division of Research and Innovation, Universiti Malaysia Pahang for funding this study (RDU Grant No: 1903126 and UIC181505).

References

Abawajy, J. (2014) 'User preference of cyber security awareness delivery methods', *Behaviour and Information Technology*, Vol. 33, No. 3, pp.236–247.

Aradea, A., Suwardi, I., Surendro, K., Mubarok, H. and Darmawan, I. (2019) 'Self-adaptive cybersecurity system', in *2018 International Conference on Industrial Enterprise and System Engineering (IcoIESE 2018)*, March, Atlantis Press.

Barclay, C. (2014) 'Sustainable security advantage in a changing environment: the cybersecurity capability maturity model (CM2)', *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World – Impossible Without Standards? K 2014*, pp.275–282.

Becker, J., Knackstedt, R. and Pöppelbuß, J. (2009) 'Developing maturity models for IT management – a procedure model and its application', *Business & Information Systems Engineering (BISE)*, Vol. 1, No. 3, pp.213–222

Boyson, S. (2014) 'Cyber supply chain risk management: revolutionizing the strategic control of critical IT systems', *Technovation*, Vol. 34, No. 7, pp.342–353.

CISA (2013) *Security Is Not Just a Technical Issue* [online] https://www.us-cert.gov/bsi/articles/best-practices/governance-and-management/security-is-not-just-a-technical-issue (accessed 11 May 2019).

De Bruin, R. and Von Solms, S.H. (2016a) 'Cybersecurity governance: how can we measure it?', *2016 IST-Africa Conference*, IST-Africa 2016, pp.1–9.

De Bruin, R. and Von Solms, S.H. (2016b) 'Modelling cyber security governance maturity', *International Symposium on Technology and Society, Proceedings*, March, pp.1–8.

De Bruin, R. and Von Solms, S.H. (2017) 'Humanitarian perspective of cybersecurity and cybersecurity governance', in *2017 IST-Africa Week Conference (IST-Africa)*, pp.1–10, IEEE.

Dutta, A. and McCrohan, K. (2002) 'Management's role in information security in a cyber economy', *California Management Review*, Vol. 45, No. 1, pp.67–87.

Fernando, Y. and Chukai, C. (2018) 'Value co-creation, goods and service tax (GST) impacts on sustainable logistic performance', *Research in Transportation Business & Management*, Vol. 28, No. 1, pp.92–102.

Fernando, Y. and Saththasivam, G. (2017) 'Green supply chain agility in EMS ISO 14001 manufacturing firms: empirical justification of social and environmental performance as an organisational outcome', *International Journal of Procurement Management*, Vol. 10, No. 1, pp.51–69.

Fernando, Y., Chidambaram, R. R. and Wahyuni-TD, I. S. (2018) 'The impact of big data analytics and data security practices on service supply chain performance', *Benchmarking: An International Journal*, Vol. 25, No. 9, pp.4009–4034.

Fernando, Y., Gui, A., Wahyuni-TD, I.S., Seo, Y.W. and Haron, H. (2019) 'Supplier sustainable integrity using a split-half method: empirical evidence from Malaysia', *KnE Social Sciences*, Vol. 1, No. 1, pp.579–592.

García-Mireles, G.A., Moraga, M.Á., García, F. and Piattini, M. (2015) 'Approaches to promote product quality within software process improvement initiatives: a mapping study', *Journal of Systems and Software*, Vol. 103, No. C, pp.150–166.

Halvorsen, C.P. and Conradi, R. (2001) 'A taxonomy to compare SPI frameworks', in *European Workshop on Software Process Technology*, June, pp.217–235, Springer, Berlin, Heidelberg.

IBM (2018) *2018 Cost of Data Breach Study: Global Overview* [online] https://www.ibm.com/downloads/cas/861MNWN2 (accessed 2 April 2019).

Jasmi, M.F.A. and Fernando, Y. (2018) 'Drivers of maritime green supply chain management', *Sustainable Cities and Society*, Vol. 43, No. 1, pp.366–383.

Khoshgoftar, M. and Osman, O. (2009) 'Comparison of maturity models', *Proceedings – 2009 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2009*, pp.297–301.

Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K. (2015) 'A survey of cyber security management in industrial control systems', *International Journal of Critical Infrastructure Protection*, Vol. 9, No. 1, pp.52–80.

Le, N.T. and Hoang, D.B. (2017) 'Can maturity models support cyber security?', *2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC 2016*, pp.1–7.

Llansó, T., McNeil, M. and Noteboom, C. (2019) 'Multi-criteria selection of capability-based cybersecurity solutions', in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, January.

Mattern, T., Felker, J., Borum, R. and Bamford, G. (2014) 'Operational levels of cyber intelligence', *International Journal of Intelligence and CounterIntelligence*, Vol. 27, No. 4, pp.702–719.

Maynard, S.B., Tan, T. Ahmad, A. and Ruighaver, T. (2018) 'Towards a framework for strategic security context in information security governance', *Pacific Asia Journal of the Association for Information Systems*, Vol. 10, No. 4, pp.65–88.

Miron, W. and Muita, K. (2014) 'Cybersecurity capability maturity models for providers of critical infrastructure', *Technology Innovation Management Review*, Vol. 4, No. 10, pp.33–39.

MITRE (2010) *Cyber Security Governance A Component of MITRE's Cyber Prep Methodology* [online] https://www.mitre.org/sites/default/files/pdf/10_3710.pdf (accessed 11 May 2019).

MITRE (2017) *Cyber Prep 2.0* [online] https://www.mitre.org/sites/default/files/publications/16-0939-motivating-organizational-cyber-strategies.pdf (accessed 11 May 2019).

Perumal, S., Pitchay, S.A., Samy, G.N., Shanmugam, B., Magalingam, P. and Albakri, S.H. (2018) 'Transformative cyber security model for malaysian government agencies', *International Journal of Engineering & Technology*, Vol. 7, No. 4.15, pp.87–92.

Pöppelbuß, J. and Röglinger, M. (2011) 'What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management', in *ECIS*, June, p.28.

Rea-Guaman, A.M., San Feliu, T., Calvo-Manzano, J.A. and Sanchez-Garcia, I.D. (2017) 'Comparative study of cybersecurity capability maturity models', in *International Conference on Software Process Improvement and Capability Determination*, pp.100–113, Springer, Cham, October.

Rogers, Z. and Choi, T.Y. (2018) *Purchasing Managers Have a Lead Role to Play in Cyber Defense* [online] https://hbr.org/2018/07/purchasing-managers-have-a-lead-role-to-play-in-cyber-defense (accessed 06/08/2019).

Schumacher, A., Erol, S. and Sihn, W. (2016) 'A maturity model for assessing Industry 4.0 readiness and maturity of manufacturing enterprises', *Procedia CIRP*, Vol. 52, No. 1, pp.161–166.

Scully, T. (2014) 'The cyber security threat stops in the boardroom', *Journal of Business Continuity & Emergency Planning*, Vol. 7, No. 2, pp.138–148.

Setty, J. (2018) *Procurement & Cybersecurity: Best Practices to Safeguard Your Organization* [online] http://www.mypurchasingcenter.com/logistics/articles/procurement-cybersecurity-best-practices-safeguard-your-organization/ (accessed 06/08/2019).

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016) 'Information security management needs more holistic approach: a literature review', *International Journal of Information Management*, Vol. 36, No. 2, pp.215–225.

Srinivas, J., Das, A.K. and Kumar, N. (2019) 'Government regulations in cyber security: framework, standards and recommendations', *Future Generation Computer Systems*, Vol. 92, No. 1, pp.178–188.

Stephens, J. and Valverde, R. (2013) 'Security of e-procurement transactions in supply chain reengineering', *Computer and Information Science*, Vol. 6, No. 3, pp.1–20.

Tooranloo, H.S., Ayatollah, A.S. and Karami, M. (2018) 'IT outsourcing through group decision-making based on the principles of interval-valued intuitionistic fuzzy theory', *International Journal of Procurement Management*, Vol. 11, No. 1, pp.96–112.

Wendler, R. (2012) 'The maturity of maturity model research: a systematic mapping study', *Information and Software Technology*, Vol. 54, No. 12, pp.1317–1339.

Wiryawan, D., Suhartono, J., Fernando, Y., So, I.G. and Gui, A. (2019) 'Malware mobile devices in Indonesia', *KnE Social Sciences*, Vol. 1, No. 1, pp.259–267.

Yusliza, M.Y., Norazmi, N.A., Jabbour, C.J.C., Fernando, Y., Fawehinmi, O. and Seles, B.M.R.P. (2019) 'Top management commitment, corporate social responsibility and green human resource management: a Malaysian study', *Benchmarking: An International Journal*, Vol. 26, No. 6, pp.2051–2078.