A Strategic Roadmap for Cybersecurity Capability Engineering across different environments

Noluxolo Gcaza[1]and Jabu Mtsweni[2]
[1] Tshwane University of Technology, Pretoria, South Africa
[1] Nelson Mandela University, Port Elizabeth, South Africa
[2] Council for Scientific and Industrial Research, Pretoria, South Africa
GcazaN@tut.ac.za
JMtsweni@csir.co.za

Abstract: Digital transformation is not without risks as the threats posed by cyber-attacks in this day and age are continually on the rise. Cyber-attacks have become pervasive and thus calling for organisations to be vigilant at all times and intentional in preserving the security of critical assets. Inopportunely, cyber-attacks are not selective in nature; as such no organisation is immune to their potential impact that often manifests in financial losses and reputational damage. This challenge gives the development of a cybersecurity capability indisputable primacy as it is relevant to all organisations that reap the benefits of interconnectedness regardless of shape, size, and environment. Be that as it may, it cannot be disputed that each business environment warrants unique consideration for cybersecurity efforts to yield effective results. While capability planning exists as a discipline, there is a lack of a consistent and coherent guide for cybersecurity capability development. This paper aims to bridge this gap by proposing an adaptable roadmap for developing cybersecurity capability following design science research. This roadmap will contribute by presenting practical and flexible guidelines for the development of a cybersecurity capability that can be employed in any business environment. This approach will leverage from an existing capability engineering framework while striving to augment the adaptability of the framework to cybersecurity.

Keywords: Cybersecurity, Capability Engineering, Strategic Roadmap

1. Introduction

The adoption of emerging technologies to optimise business processes is not without risks. As a result, over the recent years, numerous entities have witnessed an exponential increase in cyber-attacks. The threat posed by these cyber-attacks is continually calling for vigilance and proactiveness from organisations. This threat does not discriminate based on the industry or size of the organisation. On one hand, large enterprises such as Yahoo have experienced a data breach that compromised over a billion user accounts (Jalali, Siegel and Madnick, 2019). Similarly, GitHub, a web-based hosting was subjected to the largest distributed denial of service (DDoS) attack where 1.35Tbps flood of traffic resulted in major websites across large portions of the United States of America (USA) being out of action for a number of hours (Chadd, 2018).

On the other hand, cyber-attacks in Small, Medium & Micro Enterprise Businesses (SMMEs) get minimal media attention which can potentially create a false sense of security. In a recent cybersecurity survey involving over a thousand of SMMEs in the USA and United Kingdom (UK) sixty-seven percent of respondents reported having suffered a cyber-attack in the year 2018. In addition, sixty percent of the respondents that had a data breach said the cause was a negligent employee or independent contractor (Ponemon Institute, 2018).

To address the cyber-attack pandemic, developing cybersecurity capability should become a priority to all organisations that reap the benefits of interconnectedness regardless of shape, size, and environment. A cybersecurity capability is the ability to achieve a good security posture under specified standards and conditions through a combination of people, technology and processes. The development of cybersecurity capabilities is a complex matter (Martti and Limnéll, 2016). Whether at the nation state level, or in an enterprise, various factors need to be taken into consideration. Even so, proactively building a cybersecurity capability is more cost effective than a reactive approach.

Capability development exists as a discipline, however, there is a lack of a consistent and coherent guide for cybersecurity capability development. This paper aims to bridge this gap by proposing an adaptable roadmap

[1] Lead author is affiliated with two academic institutions
[2] CSIR

Citation of this paper: Gcaza, N., & Mtsweni, J. (2020, March). A Strategic Roadmap for Cybersecurity Capability Engineering across Different Environments. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (p. 187). Academic Conferences and publishing limited.

for developing cybersecurity capability following design science research. This roadmap will contribute by presenting practical and flexible guidelines for the development of a cybersecurity capability that can be employed in any business environment. This approach will leverage from existing frameworks while striving to augment the flexibility and adaptability elements of the frameworks.

The remainder of this paper presents a definition of capability in Section 2 followed by a summary of integrated capability management. In Section 4, related works are provided. Thereafter we present the proposed strategic roadmap for cybersecurity capability engineering followed by concluding remarks.

2. Capability

The most basic definition of a capability is "the ability to do something". Capability can also be defined as the "measure of the ability of an entity (department, organization, person, system) to achieve its objectives, especially in relation to its overall mission". It is also defined as "the ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks" (Jacobs, von Solms and Grobler, 2016). According to Ulrich (2010) a capability should be clearly defined to entail:

- What is being done,
- Specific outcome,
- Intent, and
- Level of uniqueness.

The definitions primarily suggest that capability hinges on a state of being *able* to achieve particular *outcomes*. Moreover, a capability should be well defined, justified with its supporting processes describing how tasks are performed.

3. Related Works

Scientific research on cybersecurity capability development is still at its infancy however it is currently gaining a lot of traction. Jacobs et al (2016) conducted a study that showed that no cybersecurity capability development framework applicable to the business domain exists. It is under this premise the authors sought to develop a framework called the Business Cybersecurity Capability Development Framework (BCCapDev framework). The framework is intended to allow business the flexibility and agility to quickly identify and develop cybersecurity capabilities. This study is a good point of departure however it fails to capture the principle of continuous improvement as part of the capability management process.

Lehto and Limnéll (2016) conducted an analysis of the cybersecurity capability in Finland using the DOTMLPF-II components: Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, Interoperability and Information. These components where chosen as the basis of the analysis because they are deemed as the core steps in building a national cybersecurity capability. The study determined recommendations to fill the capability gap identified in the analysis. The study does not seek to propose means to develop a cybersecurity capability, rather it applies DOTMLPF-II to merely analyse the gaps that are eminent in the cybersecurity capability of Finland.

Mtsweni, Gcaza and Thaba (2018) proposed a unified cybersecurity framework that addresses the complex and multifaceted nature of cybersecurity. The framework is intended for large and complex environments to define and apply cybersecurity capabilities using a systematic approach. This study is underpinned on principles of Integrated Capability Management (ICM) to demonstrate that cybersecurity is more than a mere technical issue but requires a holistic risk centred approach. Though a holistic view of cybersecurity is provided in this study, the framework does not clearly articulate the point of departure and a series of key steps to take towards the eventual capability.

Jalali, Seigel and Manick (2019) developed a simulation game to study the effectiveness of decision-makers in overcoming complexities in building cybersecurity capabilities. Analysing 1479 simulation runs, the authors compared the performances of a group of experienced professionals with those of an inexperienced control group. The findings of the study highlight the importance of training for decision-makers with a focus on systems thinking skills. The investigation lays the groundwork for future research on uncovering mental biases about the

complexities of cybersecurity. The paper is more focused on motivating the cybersecurity community to design and adopt enhanced educational and training programs that challenge entrenched mind-sets and encourage proactive cybersecurity capability development.

4. Integrated Capability Management

Integrated Capability Management (ICM) is a planning model employed in military defence environments to establish defence capabilities. This model is considered to be relevant in the cybersecurity domain for establishing capability (Mtsweni, Gcaza and Thaba, 2018). The ICM consists of four phases including Capability Definition, Capability Specification, Capability Establishment and Capability Employment as illustrated in Figure 1.

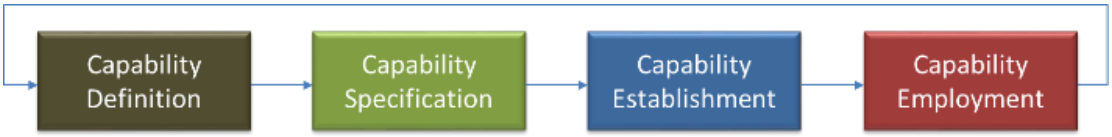

Figure 1: Integrated Capability Management *(Mtsweni, Gcaza and Thaba, 2018)*

- Capability Definition: This phase is concerned with determining the existing capability gaps and quantifying these gaps and envisaged resources. In this phase, Operational Requirements (ORs) are sought and categorised in order to disseminate appropriate services. The question addressed in this phase is *"what should the organisation be able to do to achieve its ORs?".*
- Capability Specification: This phase receives the gaps identified in the definition phase for further investigation and validation. Thereafter, functional requirements of the envisaged capability are established specifically to address the identified gaps. This phase addresses the question *"what are the typical functionalities required to enable the organisation to achieve its operational objectives?".*
- Capability Establishment: This phase focuses on establishing all the capability elements that will support the capability specifications. In this phase, the acquisition process is triggered addressing the question *"what are the capability elements required to enable the enable the organisation to support its specification and thus achieve its operational objectives?".*
- Capability Employment: This phase is concerned with the operational effectiveness of the established capability. In this phase, the question to be asked is *"How well does the established capability achieve the organisations operational goals?".*

The phases of ICM model captures the high-level route towards developing and managing a capability. As such, this model can be used to for developing a cybersecurity capability. Thus, it forms the foundation of the roadmap proposed in this paper.

5. Strategic Roadmap for Cybersecurity Capability

A roadmap is used to visualise the route toward an envisaged end. It is used in contemporary firms as a supportive framework for research and development of future technologies. In organisations, road mapping is an integral part of formulating and implementing innovation strategies (Ghobakhloo, 2018). It is therefore obvious that a strategic roadmap is indispensable for securing success in the development of a cybersecurity capability. The roadmap proposed in this study aims to be first line guidance for organisations planning to build a cybersecurity capability. Organizations need to apply the strategic roadmap to better time, visualize and understand each move and decisions that they need to make to facilitate the establishment of the capability (Ghobakhloo, 2018).

The proposed strategic roadmap for cybersecurity engineering has 4 phases namely 1) Cybersecurity Capability Definition, 2) Cybersecurity Capability Specification, 3) Cybersecurity Capability Establishment, and 4) Cybersecurity Capability Employment. Each phase has an input and output to indicate what an organisation must have accomplished at the end each phase. Figure 2 represents the proposed Strategic *Roadmap for Cybersecurity Capability Engineering.*

Citation of this paper: Gcaza, N., & Mtsweni, J. (2020, March). A Strategic Roadmap for Cybersecurity Capability Engineering across Different Environments. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (p. 187). Academic Conferences and publishing limited.

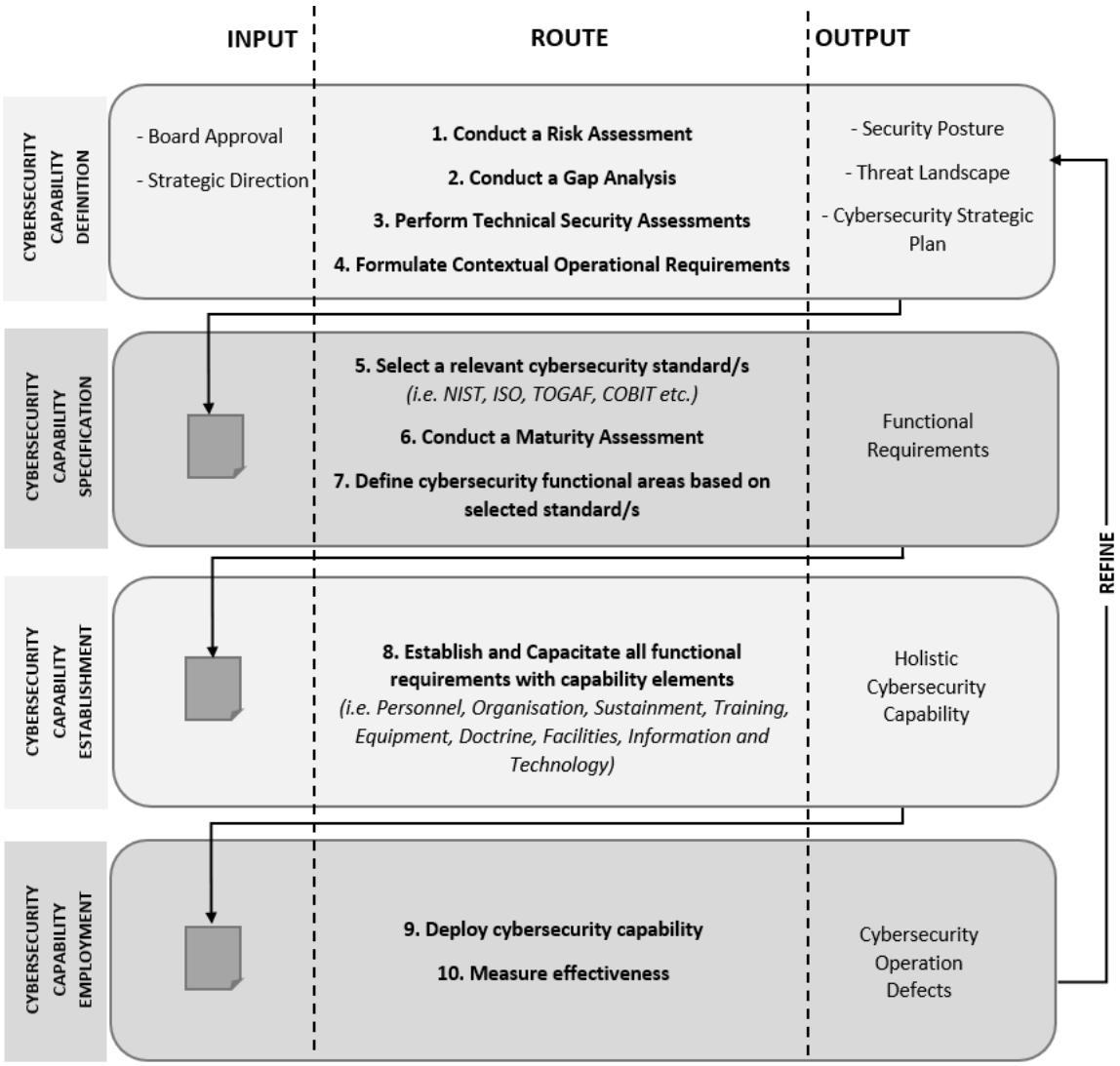

Figure 2: Strategic Roadmap for Cybersecurity Capability Engineering

5.1 Phase 1

The buy-in of the Board of Directors in defining a cybersecurity capability is paramount (von Solms and von Solms, 2018). This is critical for ensuring strategic direction were cybersecurity risks are prioritized and investments are made towards mitigation strategies. Thus, board approval and strategic direction are critical inputs to this phase. Since this phase is concerned with determining the existing capability gaps and quantifying these gaps, a number of assessments are recommended in order to establish the context of each organisation. Conducting the recommended assessments will provide the organisation with a prioritised list of security risks, and an understanding of their operating context and their vulnerabilities. It is from such context that ORs can be defined.

The Centre for the Protection of National Infrastructure (CPNI) regards ORs as the enabler for organisations to define concise and contextual high-level statement of their security needs (CPCPNI, 2013). The CPNI asserts that security capabilities that are developed without well-defined ORs are most likely to fail. Two OR levels are delineated to include Level 1 and Level 2, where the former involves assessing, evolving and justifying the actions to be taken and investments made to protect critical assets against security threats detailed in a strategic security plan. The latter receives the strategic security plan as input and derives a more detailed plan of action.

The proposed roadmap suggests that the ORs be captured in the strategic security plan and be one of the outputs of the Cybersecurity Capability Definition Phase. Other outputs include security posture and threat landscape of

the business which present the context since each business environment warrants unique consideration for cybersecurity efforts to yield effective results. It is the assertion of the authors that cybersecurity measures that are not contextual lack effectiveness.

5.2 Phase 2

The Cybersecurity Capability Specification Phase receives input from phase one to ensure that the specification addresses the ORs of the organisation. Taking those into consideration the following steps are recommended:

1. Select a relevant cybersecurity standard
2. Conduct a Maturity Assessment
3. Define functional areas

Cybersecurity standards are important because they serve as a yardstick to indicate effectiveness of a cybersecurity capability. The use of a maturity assessment will depict the level of current capacity as well as gaps that exist. Finally, once a standard is select and gaps are identified, the functional requirements can be conceived.

The National Institute for Standards and Technology (NIST) Cybersecurity Framework is by far the most popular guide for used to define functional requirements of a cybersecurity capability (NIST, 2018). The framework defines 5 core functions as depicted in Figure 3 below:

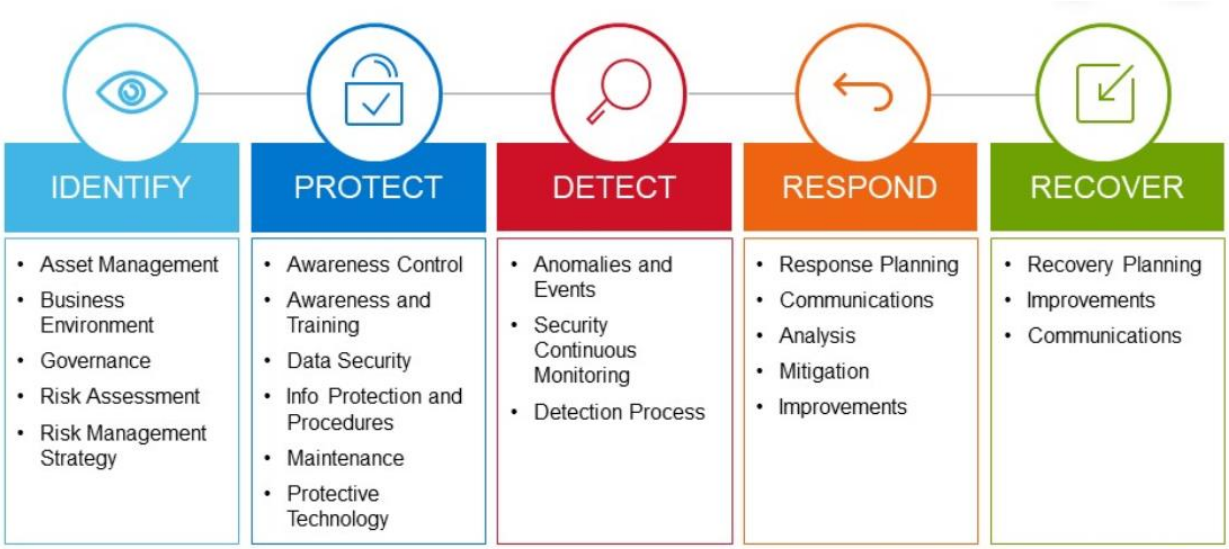

Figure 3: NIST Cybersecurity Framework

- Identify – the activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs (NIST, 2018).
- Protect – the Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology (NIST, 2018).
- Detect – this function enables the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes (NIST, 2018).
- Respond – this function focuses on the establishment of appropriate activities to do when a cybersecurity event is detected. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements (NIST, 2018).

- Recover – the Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome categories within this Function include: Recovery Planning; Improvements; and Communications (NIST, 2018).

The proposed roadmap does not insist on the NIST Cybersecurity Framework, so organisations are free to select any other standards.

5.3 Phase 3

The Cybersecurity Capability Establishment phase receives the Functional requirements as input with the aim to define the capability elements required to enable the organisation to support its specification and thus achieve its operational objectives.

According to Oosthuizen (2008) capability may be conceived of as comprising nine constituent elements namely POSTEDFIT (Personnel, Organisation, Sustainment, Training, Equipment, Doctrine, Facilities, Information and Technology). Table 1 provides a description of these elements.

Table 1: POSTEDFIT Description

Capability Element	Description
P-Personnel	Qualified human resources to support the capability, including recruiting, maintaining, staffing levels, career management, development, leadership, morality, ethos and values.
O-Organisation	The organisational structure, including size, shape, and expertise and support lines required. This includes actual organisations (order of battle and structures), organisational characteristics, responsibilities, business processes and the allocation of equipment in order to conduct an operation
S-Support	The logistic, financial and information support required including resources, support from other Services and agencies, logistic systems and mobilisation planning.
T-Training	The training required including individual, joint and combined training, training content, methods and resources (curricula, standards, equipment, simulators, funding and time) which enables performance and are in support of the mission.
E-Equipment	The type, quantity of the required defence equipment including acquisition, standardisation and compatibility, performance, maintainability, availability, reliability, robustness, flexibility, interoperability and through life support, interpretation of tests and accuracy levels, and any other guaranties that the user requires, are to be stated.
D-Doctrine	The overall governance including regulations, operating procedures and other required directives, incorporating concepts, policies, strategy (national and defence), interoperability levels, tactics, techniques and procedures which govern the how operations are conducted.
F-Facilities	The required support and training facilities such as real estate, and technical support centres.
I-Intelligence	The characteristics of defence intelligence, information, data and data processing systems required, including content, timeliness, presentation, format, reliability, compatibility, validity, data correlation and fusion.
T-Technology	The technologies required to support the capability.

Oosthuizen (2008) insists that "all capability [elements] contribute to an integrated capability; a deficiency in one [element] impacts on the capability as a whole. Thus, capability manifests itself in the emergent behaviour of its constituent elements." Some of the POSTEDFIT elements relate to the DOTMLPF-II capability building tool defined by the US Armed Forces to characterize a cybersecurity capability. Lehto and Limnell (2016) explore: Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability and Information which are described in Table 2: DOTMLPF-II Description below.

Table 2: DOTMLPF-II Description

Capability Element	Description
D- Doctrine	The fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It also refers to how the Army intends to operate and fight.
O-Organization	The order of battle and structures adopted.
T-Training	The required training to advanced individual, various types of unit training, and joint exercises.
M-Material	The equipment necessary for the effective operations.
L-Leadership	The overall professional development of leaders to lead the operations.
P-Personnel	Qualified human resources to capacitate the operations.
F-Facilities	The real estate and industrial facilities such as government owned ammunition production facilities.
I-Interoperability	The ability of the capability to offer support and to receive it from other systems to achieve efficiency.
I-Information	Information needs to support the various elements and process in the capability.

The later capability elements from US Armed Forces present Leadership, Interoperability and Information as key to supporting and developing a capability. When using the proposed roadmap, one is not limited to a particular framework for capability establishment. Rather, it recommended that an organisation applies a holistic framework to facilitate the phase in order to realise a holistic cybersecurity capability.

5.4 Phase 4

This phase encompasses verification to ensure that the established capability meets the capability specification. It is in this phase that an organisation ensures that the capability reaches the required levels of operational effectiveness. The steps involved in this phase include:

1. Deploying the security capability
2. Measuring effectiveness of the capability

Deploying the security capability advocates a shift from a formulation stage to an operational stage. The security deployment is guided by the framework that an organisation opts to adopt in Phase 3. Thus, if one of the recommended capability frameworks is adopted i.e. POSTEDFIT or DOTMLPF-II, deploying the security capability will ultimately translate to implementing the capability elements with the aim of assessing if capability specifications are being met.

To measure the operational effectiveness of the capability it is recommended to first define desirable outcomes. In this case, the outcomes should be derived from the ORs that are delineated in phase 2. According to G7 Cyber Expert Group (2017) – an international intergovernmental economic organization which consists of the seven largest advanced economies in the world, some of the desirable outcomes of a cybersecurity capability are:

- The capability elements are in place.
- Cybersecurity influences organizational decision-making.
- There is an understanding that disruption will occur.
- An adaptive cybersecurity approach is adopted.
- There is a culture that drives secure behaviours.

It is worth emphasizing that each organisation that is establishing a cybersecurity capability must define such outcomes having their context in mind. As previously mentioned, the outcomes need to be a derivative of the ORs to ensure the context at hand.

The G7 Cyber Expert Group (2017) further suggest that once the desirable outcomes are set, assessment components must be defined to facilitate continuous improvement. The assessment components comprise of:

- Establishing clear assessment objectives.
- Setting and communicating methodology and expectations.
- Maintaining a diverse toolkit and process for tool selection.
- Reporting clear findings and concrete remedial actions.
- Ensuring that assessments are reliable and fair.

Any operational deficiencies determined in this phase are channelled to the initial phase as gaps and thus creates an iterative cycle. Measuring the effectiveness of the capability is ultimate to ensure that the cybersecurity capability continuously improves to reach higher levels of maturity.

6. Conclusion

The reliance on interconnected digital technologies for critical business operations can possibly place an entity at the mercy of cybercriminals. It is for this reason that cybersecurity is prioritized at a strategic level. The losses emanating from cybersecurity incidents places a financial and reputational burden on organisations which then necessitates the development and implementation of a cybersecurity capability. This paper addressed the lack of consistent and coherent guide for cybersecurity capability development by proposing an adaptable roadmap for developing cybersecurity capability. This roadmap can serve as a practical guide to navigating the complexities of capability development.

References

Chadd, A. (2018) 'DDoS attacks: past, present and future', *Network Security*, 7(2018), pp. 13–15.

CPCPNI (2013) 'Guide To Producing Operational Requirements', p. 46.

G7 Cyber Expert Group (2017) *Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*. Available at: http://www.mef.gov.it/inevidenza/documenti/PRA_BCV_4728453_v_1_G7_Fundamental.pdf.

Ghobakhloo, M. (2018) 'The future of manufacturing industry: a strategic roadmap toward Industry 4.0', *Journal of Manufacturing Technology Management*, 29(6), pp. 910–936. doi: 10.1108/JMTM-02-2018-0057.

Jacobs, P. C., von Solms, S. H. and Grobler, M. M. (2016) 'Towards a framework for the development of business cybersecurity capabilities', *The Business and Management Review*, 7(4), pp. 51–61. doi: 10.13140/RG.2.1.5110.0406.

Jalali, M. S., Siegel, M. and Madnick, S. (2019) 'Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment', *Journal of Strategic Information Systems*. Elsevier, 28(1), pp. 66–82. doi: 10.1016/j.jsis.2018.09.003.

Martti, L. and Limnéll, J. (2016) 'Cyber Security Capability and the Case of Finland', in Koch, R. and Rodosek, G. (eds) *The 15th European Conference on Cyber Warfare and Security*. Munich: Academic Conferences and Publishing International Limited, p. 182.

Mtsweni, J., Gcaza, N. and Thaba, M. (2018) 'A unified cybersecurity framework for complex environments', in *ACM International Conference Proceeding Series*, pp. 1–9. doi: 10.1145/3278681.3278682.

NIST (2018) *Framework for Improving Critical Infrastructure Cybersecurity*. doi: 10.6028/NIST.CSWP.04162018.

Oosthuizen, R. and Roodt, J. H. (2008) 'Credible Defence Capability: Command and Control at the Core', *Land Warfare Conference*, (April).

Ponemon Institute (2018) *2018 State of Cybersecurity in Small & Medium Size Businesses*.

von Solms, B. and von Solms, R. (2018) 'Cybersecurity and information security – what goes where?', *Information*

Citation of this paper: Gcaza, N., & Mtsweni, J. (2020, March). A Strategic Roadmap for Cybersecurity Capability Engineering across Different Environments. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (p. 187). Academic Conferences and publishing limited.

and Computer Security, 26(1), pp. 2–9. doi: 10.1108/ICS-04-2017-0025.
Ulrich, W. (2010) 'Defining the Business Capability - A Cheat Sheet', *Business Architecture: The Art and Practice of Business Transformation*. Available at: https://www.bainstitute.org/resources/articles/defining-business-capability-cheat-sheet.

Citation of this paper: Gcaza, N., & Mtsweni, J. (2020, March). A Strategic Roadmap for Cybersecurity Capability Engineering across Different Environments. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (p. 187). Academic Conferences and publishing limited.