A Unified Cybersecurity Framework for Complex Environments

Jabu Mtsweni
Council of Scientific and Industrial Research
P.O. Box 395
Pretoria, South Africa
mtswenij@gmail.com

Noluxolo Gcaza
Council of Scientific and Industrial Research
P.O. Box 395
Pretoria, South Africa
ngcaza@csir.co.za

Mphahlele Thaba
Council of Scientific and Industrial Research
P.O. Box 395
Pretoria, South Africa
jthaba@csir.co.za

ABSTRACT

Information and Communication Technologies (ICTs) present a number of vulnerabilities, threats and risks that could lead to devastating cyber-attacks resulting into huge financial losses, legal implications, and reputational damage for large and small organizations. As such, in this digital transformation and 4th industrial revolution era, nations and organizations have accepted that cybersecurity must be part of their strategic objectives and priorities. However, cybersecurity in itself is a multifaceted problem to address and the voluntary "one-size-fits-all" cybersecurity approaches have proven not effective in dealing with cyber incidents, especially in complex operational environments (e.g. large technology-centric organizations) that are multi-disciplinary, multi-departmental, multi-role, multi-national, and operating across different locations. Addressing modern cybersecurity challenges requires more than a technical solution. A contextual and systematic approach that considers the complexities of these large digital environments in order to achieve resilient, sustainable, cost-effective and proactive cybersecurity is desirable. This paper aims to highlight through a single case study approach the multifaceted nature and complexity of the cybersecurity environment, pertinently in multi-disciplinary organizations. Essentially, this paper contributes a unified cybersecurity framework underpinned by an integrated capability management (ICM) approach that addresses the multifaceted nature of cybersecurity as well as the challenges and requirements eminent in complex environments, such as national government, municipalities or large corporations. The unified framework incorporates realistic and practical guidelines to bridge the gap between cybersecurity capability requirements, governance instruments and cybersecurity capability specification, implementation, employment and sustainment drawing from well-tested military capability development approaches.

CCS CONCEPTS

• **Security and privacy → Distributed systems**; *Operating Systems; Network systems; Hardware security*

KEYWORDS

Cybersecurity, Cloud Security, Security Architecture, Case Study, Integrated Capability Management

SAICSIT '18, September 26–28, 2018, Port Elizabeth, South Africa
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-6647-2/18/09..$15.00
https://doi.org/10.1145/3278681.3278682

1 INTRODUCTION

The integration of Information Communication Technologies (ICTs) in the modern day business landscape is inevitable. Organizations are relying heavily on ICTs to achieve competitive edge amongst other objectives. These organizations are operating in information rich environments, depending on a wide range of information assets. While ICTs enable simplified access, sharing and management of information assets, they also introduce a host of security vulnerabilities, threats and risks [1] In the state of cybersecurity report by ISACA [2], it is evident that cybersecurity remains dynamic and turbulent as the field continues to mature, and cyber-attacks are a threat to all kinds of enterprises. This has placed cybersecurity in the strategic agenda of many organizations both in the public and private sector, especially as cybersecurity incidents continue to impact organizations of any size and individuals of any stature.

An analysis of the South African cybersecurity incidents indicate that mostly large public and private organizations are impacted [3]. Recent examples of local large organizations that have been victims of cyber incidents include: (1) Liberty Group [4], (2) Master Deeds [5], (3) Standard Bank [6]. Globally, there are many of similar incidents affecting large corporations such as Facebook, US National State Security Agencies, and many others. It is evident that cybersecurity affects all people, organizations, and nations that have embraced the use of technology and information systems in their environments.

Traditional businesses and governmental organisations tend to rely heavily on technical, yet inherently vulnerable solutions [1] to protect their information assets and detect known cyber threats and attacks [7]. As it is, existing cybersecurity regulatory frameworks fall short of harmonizing cybersecurity best practices [8], and thus are considered to be fragmented [9]. According to [10] "today's defence in depth security models are naïve. The reliance on traditional access control, threat detection and threat protection is clearly inadequate".

Consequently, the complex nature of cybersecurity challenges cannot be adequately addressed across different and multi-faceted environments using traditional and generic approaches. For instance, technology solution such as signature-based anti-virus software may be enough in securing a small entity from known malware and indicators of compromise. However for large organizations, a completely different approach may be required, mainly because complex environments require extensive and integrated cybersecurity modalities to deal with the composite nature of cybersecurity threats and risks. It has also been argued before that technology on its own is not the answer to cybersecurity challenges in large and complex environments [11]; but a consolidated and integrated underlying structure that considers the overall organization's strategy and capabilities, skills and people, external and internal threat vectors, cost-benefit, and other factors is paramount.

Thus, in this paper we present a unified cybersecurity framework underpinned by an integrated capability management model that focuses on complex digital environments. The framework was designed based on a case study supported by a coordinated risk assessment conducted within a large public sector organization made up of different functional departments using a variety of complex and integrated information systems dealing with different portfolios managed by different domain owners and serving thousands of both internal and external stakeholders.

The rest of the paper is structured as follows: Section 2 defines the cybersecurity complex environment focusing on the definitions, building blocks and attributes of such environments. Section 3 discusses the research methodology undertaken to conduct the research presented in this paper. Section 4 discusses a selection of existing cybersecurity architectures and frameworks highlighting their implementations and possible improvements. Section 5 provides a summary of the case study findings drawn from a risk assessment conducted in a large public organization emphasizing the key components that should be considered when developing the proposed cybersecurity framework. Section 6 discusses an integrated capability management approach that is the foundation of the proposed unified cybersecurity framework presented and discussed in Section 7. The paper is summarized and concluded in Section 8.

2 CYBERSECURITY IN COMPLEX ENVIRONMENTS

The International Telecommunication Union (ITU) defines cybersecurity as a "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" [12]. Based on the definition, it is quite evident that cybersecurity is not only a technical issue; "it is a richer and more intricate problem to solve" [11]. Some researchers have also suggested that cybersecurity is more of a process and leadership issue than a technical issue [13].

In practice, the cybersecurity landscape is primarily categorized into technology, people, and processes. The technology aspect places much attention on technical solutions such as security systems and controls. On the other hand, the human-cantered point of view places emphasis on the measures that fundamentally deal with human behaviour such as awareness campaigns and educational programmes, and the processes deal with the strategies, policies and standard operating procedures. In the past, technical measures were regarded as the paramount solution to cybersecurity. Modern solutions have, to a large extent, been adopted using technical measures in isolation [14]. However, after a legacy of unsuccessful technical efforts, it became clear that, in isolation, such solutions are insufficient to mitigate cyber-related risks [14] primarily because "operational controls, in turn, depend on human cooperation, hence behaviour, as well as knowledge in order to be effective" [15].

The essence of cybersecurity is preserving the confidentiality, integrity and availability of information in the realm of cyberspace [16]. Data is now the new currency, and cyber-criminals are after information assets [17]. The confidentiality property ensures that information is available only to the users with rights and privileges to use it and that unauthorized users are prohibited from gaining access. Integrity is concerned with ensuring that information is unaltered, reliable and complete. Availability pertains to information being always available to authorized users.

Many large technology-centric organisations are identified as "complex"; however there is no widely accepted definition of a complex business environment. Rather, the concept is associated with a number of attributes that denote the complexity of the operational environment. These attributes are as follows:

- *Multifaceted organisational structure,*
- *Variety of overlapping processes and operations,*
- *Interconnected information systems,*
- *Integrated flow of information,*
- *A large size of the organisation, and*
- *Geographical spread of business units.*

One of the major challenges of cybersecurity in complex environments is the alignment of the cybersecurity programme with the overarching strategy of the organisation. In addition, the global shortages of cybersecurity skills makes the cybersecurity domain even more challenging [2], [18]. The unidentified relationship between the new systems and existing solutions also increases the complexity of the domain [19]. The fact that cybersecurity technologies are predominantly built by a few influential foreign companies, makes the cyberspace even difficult to manage. This complexity is also increased by the trends where technology now plays an influential role in geopolitics.

Additionally, the fact that it takes organizations over 6 months to even realize that their systems have been subjected to cyber incidents present another complex challenge *(how do you protect what you do not know or monitor?)* [20]. In many environments, security has also been proven to be "an after-thought" – organizations do not know how to prioritize and many approach security by Fear, Uncertainty and Doubt (FUD). In our view, this multifaceted cybersecurity conundrum must be viewed from a contextual and systemic perspective [11], without ignoring that there can never be full-proof (100%) security in any environment.

3 RESEARCH METHODOLOGY

A practical research method that was adopted and used in this study in order to understand the cybersecurity posture and challenges within complex environments was a single case study [21]. The case study was chosen as it provides the setting to study and understand a phenomenon in real-life setting using various data collection techniques such as semi-structured interviews, surveys, and indirect observations.

For the case study, a large public organization was studied *(the identity of the organization will remain anonymous due to ethical clearance and confidentiality requirements).* An online survey was used to collect preliminary information about the critical information systems and current cybersecurity strategy. The targets for the survey were only ICT systems owners or managers. At least 10 surveys were completed. Thereafter, a thorough risk assessment was conducted using the Facilitated Risk Analysis and Assessment Process (FRAAP) [22] with the purpose of identifying critical information systems (risk profiling), including understanding current processes and strategies including "as-is" cybersecurity posture and maturity levels.

The rationale behind using FRAAP is that it is a work-session based approach and was found to be an efficient methodology for identifying, examining and documenting risks. This process relies on the subject matter specialists and users who are familiar the environment and associated information system resources. It also relies on staff members who have understanding of the system's vulnerabilities and related controls.

The risk assessment was conducted with the 10 participants that completed the surveys. It is worth noting that these participants had great knowledge and experience in the ICT environment of the organization, and most have been in the organization for a number of years.

4 CYBERSECURITY REGULATORY FRAMEWORKS

There is a spectrum of voluntary and regulatory IT governance, information security governance and cybersecurity frameworks catering for different cybersecurity guidelines and controls. Research suggests that these frameworks are not extensive and adequate [23] to deal with the forever changing IT and cybersecurity landscape. As a result, most organizations, particularly large ones, use these artefacts for compliance purposes and in other cases; these frameworks are used as "check-boxes". It is also worth noting that most of these common IT governance and security frameworks are touted by international organizations for all environments, but at times they may not be fully relevant to organizations in local and yet complex environments. Some of the frameworks reviewed include: (1) NIST Cybersecurity framework, (2) ISO 270001, (3) Gartner Adaptive Security Architecture, (4) COBIT5, (4) and TOGAF. Generally, cybersecurity frameworks are quite extensive and complex [9]. Thus, only the applicable and widely used frameworks were analysed for this study. These frameworks are discussed below in the context of their applications to complex environments as per the focus of this research study.

4.1 NIST Cybersecurity Framework

The National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) is a prioritized, flexible, and voluntary framework that provides standards, guidelines, and best practices to assess and manage cybersecurity-related risks in private-sector organizations [24]. It can also be applied in small and public-sector organizations (mostly only outside the US), and it encourages proactive cybersecurity.

CSF core functions are grouped into five categories as depicted in Fig. 1. These are: (1) Identify – provides guidelines for understanding the business environment, organizational assets, conducting risk assessments and managing the whole cybersecurity governance strategy. (2) Protect – details technical and practical ways of protecting the business environment, information assets, and people. (3) Detect – suggests processes for detecting anomalies and security events, in an organization and conducting continuous security monitoring. (4) Respond – describes approaches to incident response planning, incident response management, including how to engage with stakeholders, preserve digital evidence, and make improvements towards incident response. (5) Recover– provides guidelines on how to recover from cybersecurity incidents through proper recovery planning, gap remediation, and proper communication.

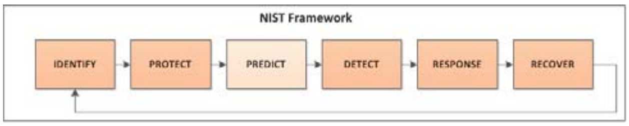

Figure 1: NIST cybersecurity framework.

One category that is not part of the framework is "Predict", which in our view, is quite critical especially in this day-and-age where adequate and proactive security of information assets cannot be realized without threat intelligence. It is because of this background that we have included the function in the framework.

Some of the limitations that have been observed with the framework when applied in complex environments include lack of consideration for budget, cost-benefit analysis, and existing infrastructure, including prioritization of capabilities and who is responsible for the different cyber capabilities in an organization.

4.2 ISO 27001

ISO 27001 (previously called ISO/IEC 27001:2005) is a framework for an information security management system (ISMS) [25][26]. An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. ISO 270001 as the widely used standard within the information security domain [26] and has a main objective of supporting and guiding organizations (of any size and shape) to keep their information assets secure. It includes people, processes and IT systems by applying a risk management process.

Similar to the NIST CSF, applying the ISO 27001 requires extensive expertise and knowledge. In addition, getting such a framework to work seamlessly in complex environments can take more time, especially considering that ISO is not so easy to understand and use without strong cybersecurity knowledge [26]. The element of costs is often neglected by the ISO 27001 including the cybersecurity capacity required to implement such a framework.

4.3 Gartner Adaptive Security Architecture

Gartner introduced an adaptive security architecture in 2017 [27] that focuses on continuous security rather than incident-based response security. The architecture has four domains, some similar to the NIST CSF. These are: (1) Detect (2) Prevent (3) Respond and (4) Predict as depicted in Fig.2 below.

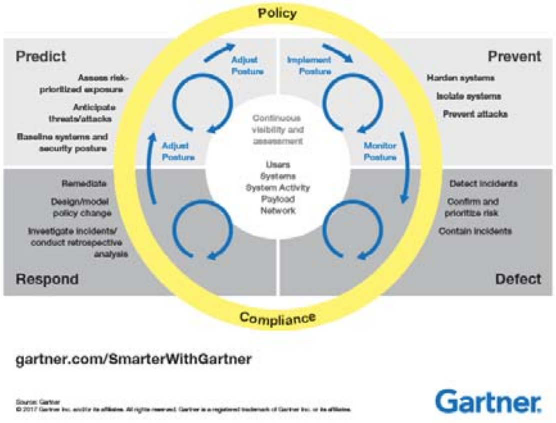
Policy
Predict
Assess risk-prioritized exposure
Anticipate threats/attacks
Baseline systems and security posture
Prevent
Harden systems
Isolate systems
Prevent attacks
Adjust Posture
Implement Posture
Adjust Posture
Monitor Posture
Continuous visibility and assessment
Users
Systems
System Activity
Payload
Network
Remediate
Design/model policy change
Investigate incidents/ conduct retrospective analysis
Respond
Detect incidents
Confirm and prioritize risk
Contain incidents
Defect
Compliance
gartner.com/SmarterWithGartner
Source: Gartner
© 2017 Gartner Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner Inc. or its affiliates.
Gartner.

Figure 2: Gartner Adaptive Security Architecture

The key differentiator in the Gartner's security architecture to other existing ones is that it focuses on continuous visibility and assessment of the security environment with policy and compliance taking a central stage. However, the architecture is limited in a sense that it also does not consider all key elements that could impact the cybersecurity posture of complex organizations, such as skills, costs, budget, and contextual threat intelligence.

4.4 COBIT 5

The Control Objectives for Information and Related Technology (COBIT) framework is created and promoted by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA) [23]. It consists of a set of best practices for IT management, and is generally adopted by the IT community. In its general form, it is meant to be Version 5 of the framework referred to as COBIT 5. It includes aspects of information security in relation to how they can be applied in real-life using the defined principles to ensure quality, control, and reliability and information security of IT systems in an organization. As a framework it is quite detailed, consisting of 34 high level objectives with over 215 control objectives. These are categorized into four domains: (1) Plan (2) Organize, (3) Acquire, and (4) Implement, deliver, support, monitor and evaluate. By design, COBIT is technology-centric with limited focus on cybersecurity, and does not pay adequate attention to people and cost-benefit analysis.

4.5 TOGAF Enterprise Security Architecture

The Open Group Architecture Framework (TOGAF) is an end-user and collaborative driven organization involved in comprehensive approaches, methodologies and supporting tools for organizing and managing technology, ensuring that projects meet businesses objectives through systematic with repeatable processes. Although TOGAF focuses on enterprise architectures, TOGAF-9 does provide an Enterprise Security Architecture for unifying services that enable the implementation of policies, standards, and risk management in an environment [28].

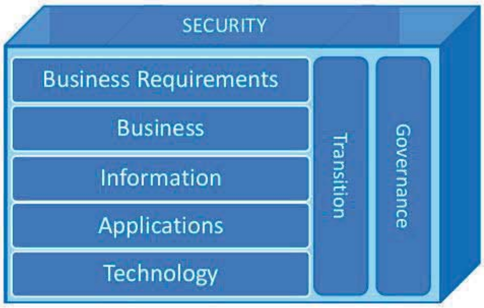

Figure 3: TOGAF Enterprise Security Architecture

As demonstrated in Fig 3, governance plays a central role in the security of the organization when applying TOGAF. The architecture composes different elements focusing on business requirements, information, applications, and technology. The architecture is useful when considering security into an enterprise architecture project and as such TOGAF-9 recommends bringing a security architect into the project as early as possible [28]. The architecture further indicates areas that should be of concern to the security architecture such as authentication, authorization, auditing, assurance, availability, asset protection and risk management.

For the purposes of this paper, TOGAF is not fully aligned, but some of its elements may be used in the proposed unified cybersecurity framework.

5 CASE STUDY FINDINGS

6.1 Risk Assessment

A risk assessment was conducted on a selection of critical information systems existing studied environment. Because the environment studied is complex by design and role, it was not feasible to assess all information systems or engage with all stakeholders. The findings highlighted below are based on online surveys, semi-structured interviews with 10 domain or system owners, and indirect observations during the risk assessment exercise. In order to verify the findings, debriefing sessions were also conducted with technology decision makers in the environment.

In this large complex environment, numerous cybersecurity risks were identified in each environment together with associated root causes. However, after a thorough analysis, the pain points in each environment were consolidated into seven risks to provide a unified cybersecurity posture for the environment.

It is worth noting that even though this large and complex environment had a spectrum of cybersecurity solutions, including paying huge license fees to vendors, the cybersecurity capability was still at maturity indicator level 1 (MIL1) based on the Cybersecurity Capability Maturity Model (C2M2) [29]. At this level, organizations cybersecurity best practices are performed in an ad-hoc and reactive manner, not in line with their own strategy and governance instruments.

The summary of risks prevalent in this complex environment despite huge technology investments in this environment are captured in Table 1.

Table 1: Extract of identified risks

#	Identified Risks
1	Unpatched and outdated software
2	Inadequate data and application lifecycle management and protect
3	Limited protection of personal information
4	Limited cybersecurity capability and capacity
5	Inadequate authorization and authentication management
6	Lack of cybersecurity awareness and training
7	Limited cybersecurity governance and instruments

Based on the risk assessment, it is quite evident that in complex environments, technology alone is not the solution. Even though this environment had patch management solutions, they still had unpatched and outdated software during the case study. This is caused by a number of factors, such as legacy applications still being used in the organization, and incompatible applications with the patch management solution. Furthermore, it was also determined that in this large business, it was difficult to manage data and applications, especially when they are under the authority of different stakeholders. This again confirmed the suggestion by [9] that cybersecurity is not necessarily an IT problem, but a leadership issue.

It is also interesting that organizations still continue to ignore protection of personal information even at the helm where governments are introducing legislations that have serious ramifications for organizations that do not secure personal information under their custodianship. In this environment, it was also evident that personal information is not adequately protected. This was determined in some instances where personal information was shared with third-parties without any governance processes in place. This was further confirmed by the processes that were in place to manage authentication and authorization to sensitive business processes.

The cybersecurity skills gaps was evident in this large environment, and this presents a number of risks because an organization cannot relegate their cybersecurity responsibilities to just technology. Without trained and skilled workforce, any security technology is bound to fail. This also touches on the aspect of cybersecurity awareness and training to the general ICTs users in the organizations. Research studies continue to suggest that the human-factor still remains the weakest link when it comes to cybersecurity breaches [14], [30].

In this large and complex environment, a gap analysis pertaining to their cybersecurity governance framework was also conducted using a combination of the cybersecurity frameworks highlighted in Section 4, and it was found minimum cybersecurity policies that a large organization need to least have in place were either missing, fragmented or incomplete. It is therefore also worth noting that without a sound and strong cybersecurity governance framework, it is near impossible to adequately secure a complex environment.

6 INTEGRATED CAPABILITY MANAGEMENT

Due to increasing cybersecurity spending and constrained budgets in organizations [2] and difficulties in determining Return on Investments (ROI) on cybersecurity technologies, decision-makers can no longer afford to throw money at every cybersecurity problem. In today's cybersecurity complex environment, replacing older systems with new ones without understanding the full-picture will not solve the security problem [31]. There is therefore an urgent need in complex environments to effectively and continually re-evaluate their cybersecurity capability requirements to optimize the utilization of current and future systems [31].

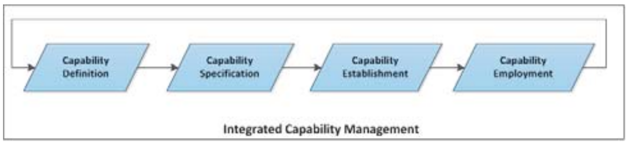

Figure 4: Capability Life Cycle [32].

Fig. 4 depicts a high-level Capability Life Cycle (CLC) that is predominately used in the South African Defence Force environment to understand, define, establish, employ, revitalize, and sustain defence capabilities across multi-disciplinary domains [32]. Simply put, a capability is defined as the "ability to do something" [32], and distinctly "it is the ability to achieve a desired affect under specified standards and conditions through a combination of means and ways" [33].

In capability-based planning, the CLC is generally followed, and this process can be coordinated using a unique integrated capability management (ICM) approach [32]. The ICM model follows an iterative and systematic process that ensures that before any defence capability is introduced into the complex defence environment, it must be fully defined and specified using various techniques, but mostly system engineering processes [34].

It is our submission that ICM is also relevant in the cybersecurity domain, particularly in underpinning any cybersecurity framework that attempts to consolidate capabilities in this complex domain. In cyber, ICM could be helpful in assisting and supporting large organizations to better understand, and effectively integrate the total enterprise's cyber capability and capacity to seamlessly secure and proactively protect the organization.

Capability management in a sense is a high-level integrative management function and aims to balance interrelated factors in meeting current operational requirements, with the sustainable use of current capabilities, and the development of future capabilities, to meet the sometimes competing strategic, operational, and tactical objectives of an organization.

In an organizational setting, cybersecurity is also considered a capability that enables the business to understand, protect, and monitor their cyber assets. This capability is composed of three elements: *people, technology and processes.* These elements are essential in achieving the desired cybersecurity effect, such as resilience, hardened systems, and strong cybersecurity posture. However, these three elements are not sufficient for providing the overall cybersecurity picture in complex environments. For instance, most of the existing cybersecurity frameworks are silent on the elements such as *environment, supporting systems and budget* and this has the potential to constrain the desired effect of the cybersecurity capability in complex environments.

In the military environments, a capability is conceived of as comprising nine POSTEDFIT-B (Personnel, Organization, Sustainment, Training, Equipment, Doctrine, Facilities, Information and Technology enabled by the Budget) constituent elements or dimensions [31]. These elements are critical towards the employment and sustainability of any capability in any complex environments. They are practically used in the South Department of Defence, UK Ministry of Defence, and US Department of Defence in different shape and form [35]. As may be noted, the POSTEDFIT elements also cover people, technology and processes (i.e. doctrine). As such, it is our view that the POSTEDFIT-B elements could improve the cybersecurity environment. These elements are discussed in the context of the proposed cybersecurity framework in Section 7.

7 A UNIFIED CYBERSECURITY FRAMEWORK

In order to improve the cybersecurity posture of complex organizations, a holistic approach is necessary to achieve adequate security and resilience. A holistic view is not confined to either ends of the technical and non-technical spectrum. Instead, a holistic view of cybersecurity considers both technical and human-centred measures with the aim of establishing both resilient operational controls and competent users who appreciate their role in the security process [9], but also considers the environment, budgetary considerations and decision support. A unified cybersecurity framework requires "technical controls, governance, resilience measures, consolidated reporting, context expertise, regulation, and standards" [11]. It is evident that a coordinated, proactive approach to address this complex challenge is essential.

Principally, this paper contends towards unified cybersecurity framework that addresses the multifaceted nature of cybersecurity as well as the challenges and requirements eminent in complex environments. The unified framework provides technical, business, leadership, and human-oriented guidelines to bridge the gap between cybersecurity capability requirements, governance instruments and cybersecurity implementation particularly in complex environments.

Fig. 5 presents an overview of the proposed unified cybersecurity framework (U-CSF), which is based on the ICM approach supported by POSTEDFIT-B elements. The framework is also inspired by the risk assessment findings from the case study.

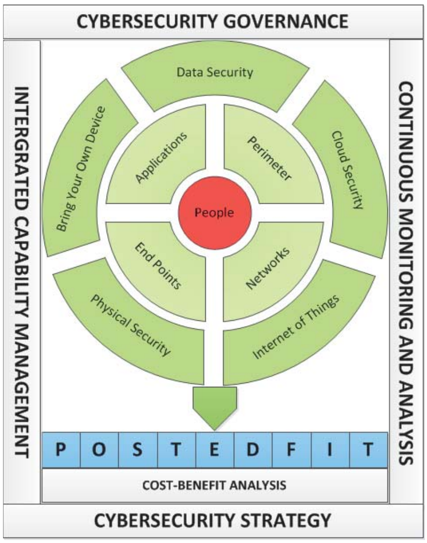

Figure 5: Unified cybersecurity framework for complex environments. © Jabu Mtsweni

As shown in Fig. 5, the U-CSF defines key elements that need to be considered when establishing and employing a cybersecurity capability in complex environments. The inner nucleus of the U-CSF focuses on *people*. As may be noted in the U-CSF, the first line of defence should be the *people*, and this means training and awareness on cybersecurity, but including scenario-planning where people know how to respond to different cybersecurity scenarios. The inner layers covering the people in the nucleus of the U-CSF focuses on the technical security aspects and these are the *perimeter and end point defences, network and applications security*. These are common in almost all cybersecurity architectures. The NIST CSF [24] and Gartner's adaptive cybersecurity architecture [27] provide good guidelines in implementing the technical functions of the cybersecurity capability. As such the U-CSF also adopts components from existing frameworks.

The outer layers of U-CSF nucleus include other pertinent elements that are often overlooked by existing frameworks, and these include: *physical security, Internet of Things (IoTs) and BYOD (Bring Your Own Devices) security, and Cloud and Data security*. These elements come with the new wave of digital transformation and present various challenges to traditional security approaches. For instance, complex environments need to have mechanisms in place to monitor BYOD and IoTs that permeate the environment on daily basis. These could present potential security breaches in organizations if they are not factored in the cybersecurity capability planning. In most cases, these are ignored because they are not visible to the security teams, and ordinary users can just "plug-and-play" with them in the corporate network without notice. Another important element not to ignore is physical security. *Physical security* is not separate from cybersecurity. An organization might have strong cybersecurity, but if physical security is weak, then the whole security of the organization can be compromised. It is therefore critical that complex environments pay attention to this aspect and not only in relation to the business security, but IT systems and people security.

The cyberspace is also dominated by data and cloud services, and large organizations are to some extent using these, for example: Dropbox, Google Drive, Social Media etc. However, most of these are hardly factored into the security plans of organizations. In complex environments, it could even be more challenging where users may randomly use these services to even store or share sensitive business and personal information. As such, complex environments need to consider the data and cloud security from the onset and manage accordingly following existing best practices [36].

The U-CSF posits that the *Cybersecurity Strategy and Governance* are the two strong pillars that need to support the whole cybersecurity capability in large organizations. In addition to this, the *ICM approach and continuous monitoring* and analysis of cybersecurity events need to be the order of the day in large and complex environments. Cybersecurity is not a periodical activity, but must be active and monitored 24/7. However, because there are never adequate resources to perform all cybersecurity functions all the time, the capability management approach needs to be adopted so as to prioritize and manage the risks and activities.

One of the missing links in most complex environments when deploying cybersecurity capabilities is the *cost-benefit analysis*. In large public organizations, decision-makers often do not have enough information about the technical abilities of various technologies that are being sold as "panacea" by vendors. They often adopt technical solutions without understanding the problem or the cost-benefit. In the studied environment, it was evident that there is a huge-spend on cybersecurity technologies, but the returns are not always aligned to the current spending. It is therefore our proposal that the U-CSF must incorporate the aspect of *cost-benefit analysis*, and not only from the availability of budget for cybersecurity, but on the value and returns that the technology brings in improving the cybersecurity posture. The cost-benefit analysis should not only be restricted to the technology, but also to the skills and other aspects, because large organizations may at times be overly paying for cybersecurity experts, without the real benefits. There are different ways of conducting cost-benefit analysis, but this can also be determined through rigorous risk assessment that identifies cyber risks for the organizations including potential impact and severities.

When a cybersecurity capability is established within a complex environment, POSTEDFIT-B elements must be interrogated to the fullest for a cost-effective, hardened, resilient, and proactive cybersecurity capability. The elements are related to the U-CSF in Table 2.

Table 2: Lines of Development (POSTEDFIT-B)

Element	Relevance
***P**-Personnel*	For any capability to be effective and sustainable, qualified resources to support the capability are important. This include maintaining such resources, recruiting correct skills, career development, and leadership.
***O**-Organization*	The structure and nature of the business need to be considered when establishing and maintaining the cyber capability. This will include aspects such as the size, shape, culture, processes, etc.
***S**-Support*	The cyber capability cannot be effective without organizational, logistical, infrastructural, informational, and financial support. These need to be honestly considered when deciding on establishing or improving the capability.
***T**-Training*	Individuals, departmental, and organizational training must not be ignored during the capability planning process. Factors that need to be considered in this element may include training content, methods and resources required to train the people so as to enable adequate performance of the capability. Also training needs to be dynamic and adaptive and suit the forever changing cyber environment.
***E**-Equipment*	Over and above technology, the equipment required supporting the capability need to be factored in, and this may include physical security equipment and telecommunication equipment and so forth.
***D**-Doctrine*	This element can be likened to governance including regulations, operating procedures, policies and strategies that must be in place to affect the cyber capability in a complex environment.
***F**-Facilities*	A cyber capability cannot exist in the "space", but needs to also be housed in some physical space is accessible and secure. As such during a cyber capability planning activity, facilities should be considered, and this may include facilities for servers, digital forensics, operations centres, and data centres.
***I**-Intelligence*	A cyber capability without threat intelligence is not enough. It is therefore important that information, data, data processing systems, knowledge management systems, are always available to support the cyber capability and enable continuous improvements and predict future cyber incidents.
***T**-Technology*	When deploying the cyber capability, it is important to identify the characteristics of both commercial and open source technologies required to enable a secure cybersecurity environment. Furthermore, research and development of future technologies is important, including understanding technology growth paths, cycles, and trends. The reliability, cost effectiveness, technical opportunities and risks of every technology need to be identified early-on in the capability planning process through benchmarking, proof of concepts, and comparative studies.
***B**-Budget*	All of the above elements are impossible to achieve in complex environments without adequate budget. It is therefore pertinent that the budget is set upfront when establishing a cyber capability so that prioritization can be done.

The proposed framework presents that holistic-view of employing a cybersecurity capability in complex environments. Based on the elements included in the framework, it is obvious that cybersecurity is more than a technical issue, and is also not merely an IT systems challenge. It requires a consideration of various factors that are not operating in isolation, but are integrated, interrelated and inseparable, requiring qualitative, quantitative, subjective, objective and risk-based interventions so as to achieve the desired effects.

8 CONCLUSIONS

Cybersecurity is an ecosystem; and threats are too complex and dynamic for organizations to manage all risks and vulnerabilities in a timely and agile manner. It is based on this premise that the U-CSF is put forward in this paper. It is envisaged that this model could assist large and complex environments to define and apply their cybersecurity capabilities in a systematic approach that also considers the overall business environment. This model can also be applied in simpler environments, but is envisaged to address some of the challenges that are experienced in complex environments. Due to the scope of the research presented in this paper, the framework has not been tested in a real-life environment as of yet, and for further research this is being considered including conducting additional case studies in other large and complex environments.

REFERENCES

[1] Y. Younan, "25 Years of Vulnerabilities: 1988-2012," 2013. [Online]. Available: https://courses.cs.washington.edu/courses/cse484/14au/reading/25-years-vulnerabilities.pdf. [Accessed: 01-Sep-2018].

[2] ISACA, "State of Cybersecurity," 2018. [Online]. Available: https://cybersecurity.isaca.org/state-of-cybersecurity. [Accessed: 01-Sep-2018].

[3] B. Van Niekerk, "An analysis of cyber-incidents in South Africa," *African J. Inf. Commun.*, vol. 20, pp. 113–132, 2017.

[4] T. Shapshak, "Liberty hack the 'biggest breach yet,'" *Financial Mail*, 21-Jun-2018.

[5] P. Fihlani, "Millions caught in South Africa's 'worst data breach' - BBC News," *BBC News*, 2017.

[6] G. van Zyl, "Standard Bank computer was hacked in R300m ATM fraud hit," *Fin24Tech*, 30-Jun-2016.

[7] J. Mtsweni, N. Shozi, K. Matenche, and M. Mutemwa, "Development of a semantic-enabled cybersecurity threat intelligence sharing model," in *11th International Conference on Cyber Warfare & Security*, 2016, pp. 244–252.

[8] S. J. Shackelford, S. Russell, and J. Haut, "Bottoms up: A Comparison of Voluntary Cybersecurity Frameworks," *UC Davis Bus. Law J.*, vol. 16, 2015.

[9] S. Tisdale and R. Morris, "Architecting a cybersecurity management framework," *Issues Inf. Syst.*, vol. 17, no. IV, pp. 227–236, 2016.

[10] P. German, "Face the facts – your organisation will be breached," *Netw. Secur.*, vol. 2016, no. 8, pp. 9–10, Aug. 2016.

[11] P. A. . Williams and A. . Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Med. Devices (Auckland, NZ)*, vol. 8, no. 2015, pp. 305–316, 2015.

[12] ITU, "Definition of Cybersecurity - ITU-T x.1205," *International Telecommunciation Union*, 2018. [Online]. Available: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. [Accessed: 01-Jul-2018].

[13] S. Tisdale, "Architecting a Cybersecurity Management Framework: Navigating and Traversing Complexity, Ambiguity, and Agility," 2016.

[14] S. Pfleeger and D. Caputo, "Leveraging behavioral science to mitigate cyber security risk," *Comput. Secur.*, vol. 31, no. 4, pp. 597–611, 2012.

[15] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[16] E. Wheeler, *Security Risk Management: building an information security risk management program from the ground up*. Elsevier, 2011.

[17] J. Mtsweni, M. Mutemwa, and N. Mkhonto, "Development of a cyber-threat intelligence-sharing model from big data sources," *J. Inf. Warf.*, vol. 15, no. 3, pp. 56–68, 2016.

[18] B. Rafferty, "Dangerous skills gap leaves organisations vulnerable," *Netw. Secur.*, vol. 2016, no. 8, pp. 11–13, 2016.

[19] C. de Waal, "Understanding the Complexity of Systems by Using the Concept Interface Matrix (CIM).," in *10th SA INCOSE Conference 2013 Systems Engineering* , 2013.

[20] C. Osborne, "Most companies take over six months to detect data breaches | ZDNet," *ZDNet*, 2015. [Online]. Available: https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/. [Accessed: 02-Jul-2018].

[21] R. K. Yin, *Case Study Research - design and methods*, 4th ed. SAGE Publications, 2009.

[22] T. Peltier, *Information security risk analysis*. 2010.

[23] S. Sahibudin, M. Sharifi, and M. Ayat, "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations," in *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, 2008, pp. 749–753.

[24] L. S.-S. Law. and undefined 2013, "NIST Cybersecurity Framework: Overview and Potential Impacts, The," *HeinOnline*.

[25] International Organization for Standardization, "ISO/IEC 27001 Information security management," *ISO*, 2018. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Accessed: 02-Jul-2018].

[26] M. . Talib, M. El Barachi, A. Khelifi, and O. Ormandjieva, "Guide to ISO 27001: UAE case study.," *Issues Informing Sci. Inf. Technol.*, vol. 7, no. 2012, pp. 331–349, 2012.

[27] R. van der Meulen, "Build Adaptive Security Architecture Into Your Organization," *Gartner*, 2017. [Online]. Available: https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/. [Accessed: 03-Jul-2018].

[28] L. Ertaul, A. Movasseghi, and S. Kumar, "Enterprise Security Architecture in TOGAF-9."

[29] W. Miron and K. Muita, "Cybersecurity capability maturity models for providers of critical infrastructure," *Technol. Innov. Manag. Rev.*, 2014.

[30] B. K. Wiederhold, "The Role of Psychology in Enhancing Cybersecurity," *Cyberpsychology, Behav. Soc. Netw.*, vol. 17, no. 3, pp. 131–132, Mar. 2014.

[31] R. Oosthuizen and J. Roodt, "Credible defence capability: command and control at the core," in *Land Warfare Conference*, 2008.

[32] M. Thaba, "Technology support for military capability based acquisition," in *International Association for Management of Technology IAMOT 2017 Conference Proceedings*, 2017.

[33] C. Smith, R. Oosthuizen, H. Harris, … J. V.-S. A. J., and U. 2012, "System of systems engineering: the link between operational needs and system requirements," *South African J. Ind. Eng.*, vol. 23, no. 2, pp. 47–60, 2012.

[34] C. J. Smith and R. Oosthuizen, "Applying Systems Engineering Principles Towards Developingg Defence Capabilities," in *22nd Annual International Symposium of the International Council on Systems Engineering, INCOSE 2012 and the 8th Biennial European Systems Engineering Conference 2012, EuSEC 2012 (2012)*, 2012, vol. 22, no. 1, pp. 1056–1070.

[35] P. C. Jacobs, S. Von Solms, and M. M. Grobler, "Towards a national cybersecurity capability development model," in *16th European Conference on Cyber Warfare and Security (ECCWS)*, 2017.

[36] R. Krutz and R. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley Publishing., 2010.