

Measuring Cybersecurity Wellness Index of Critical Organisations

Husin JAZRI¹, Omar ZAKARIA², Edmore CHIKOHORA³

^{1,3} *Namibia University of Science and Technology, No.5 Storch Street, Windhoek, Namibia*
Tel: +264 81 667 1869, Email: ¹*hjazri@nust.na* ³*echikohora@nust.na*

² *National Defence University of Malaysia, Sungai Besi Camp, Kuala Lumpur, Malaysia*
Tel: +60 12 918 0186, Email: *omar@upnm.edu.my*

Abstract: The concept of wellness in cybersecurity has not been widely discussed and this perspective is still new to date. In this paper we will discuss on this concept of cybersecurity wellness and the ability to generate an index of critical organisations through measuring cybersecurity wellness vital signs. The definition of Critical Organisation is also briefly discussed. Qualitative research using Constructive Research Approach was chosen on 20 critical organisations through a purposeful sampling and evaluated using the framework developed. Index scorecard of all cybersecurity vital signs of each organisations were collected and measured using Likert Scale value from zero to three. A composite index was then generated for each sampling organisations and group index were also computed using all 20 organisations to demonstrate the ability of measuring cybersecurity wellness of one and many organisations. The application of this research work can be used to measure the cybersecurity wellness index of critical sectors of the industry, as well as comparative analysis at national and international levels if applied accordingly.

Keywords: Cybersecurity Wellness, Cybersecurity Index, Cybersecurity Vital Signs, Critical Organisations

1. Introduction

The concept of wellness originates from an ancient root and has gained acceptance when the writings and leadership of an informal network of physicians and thinkers shaped the way we conceptualize and discuss about wellness today. The origins of wellness, however, are far older, even goes back to ancient Ayurveda in 3000 BC [1].

Referring to the World Health Organisation's definition of "health," wellness is defined as a state of complete physical, mental, and social well-being. It goes beyond mere freedom from disease or infirmity and emphasizes the proactive maintenance and improvement of health and well-being [1]. As for this research, we are not referring to wellness in the context of physical health but rather organisational health and its outlook. The relationship between organisational health and wellness is that organisation wellness is the outcome of organisation health [2]. Thus, we intend to apply the essence of organisational wellness into the context of cybersecurity wellness of organisation by identifying and measuring key cybersecurity vital signs existed in any critical organisation. Critical organisation is defined as "legal organisations or companies, whether they are government owned, public listed, private companies or non-governmental organisations that are directly or indirectly critical to the security, economy, public safety and societal well-being of any nation". Basically it includes all organisations that are defined as Critical Infrastructure (CI) organisations plus all relevant organisations that support CI organisations and those companies and/or organisations where its services deem critical to security, economy, public safety and societal well-being [3].

The term cyberwellness was first introduced by the ITU in its publication in 2015 [4]. The publication was on a project to develop and promote a metric of cybersecurity index and cyberwellness profiling among its member countries [4]. We have also observed that there was no formal definition and interpretation offered by the ITU to define and explain the term cyberwellness. Instead the published ITU framework directly applies its framework methodology using five factors to profile cyberwellness status of its member countries [4]. Thus in this paper, we intend to define and focus more on cybersecurity wellness concept and provide our interpretation to its meaning and possibly lay out all key elements that can be associated with this cybersecurity wellness. Our definition and interpretation of cyberwellness may not necessarily be the same as what the ITU has in its project document.

2. Objectives

The objective of this research paper is to introduce a concept of cybersecurity wellness for Critical Organisation [3] and to propose a measurement index on this cybersecurity wellness by analysing vital signs of these Critical Organisations. This cybersecurity wellness index can be used to evaluate the wellness of one organisation, for comparison between organisations, evaluating the wellness of group of organisations, measuring the performance of critical sectors as well as at national level using a bottom-up approach.

3. Methodology

The methodology selected for this research is qualitative approach, particularly using Constructive Research Approach [5] as a guiding step to develop the framework. The choice of this methodology is because it can help to find a solution for a real problem and at the same time provide guidance in producing a good academic paper and further research works. A proposed framework was developed and used for evaluating the cybersecurity wellness of each of sampling organisations. Purposeful sampling [6] was used to select 20 Critical Organisations that fall within the defined criteria as per its definition mentioned earlier. Semi-structured interview [6] and focus group discussion [6] were used in collecting data on cybersecurity vital signs, validating them and evaluating them using Likert Scale [6]. Accumulated Likert Scale value of all the vital signs made up a accumulated cybersecurity wellness scorecard after deduction of penalty points from Trap Case Scenario. A Trap Case Scenario is a situation whereby the penalty of 50 points was issued to organisations that are not consistent with reality check as shown in the **Figure 1**. For instance, organisation is having zero cybersecurity incidents when in reality no formal incident response team was ever set up. **Figure 2** describes the expression to calculate Cybersecurity Index. **Figure 3** derives Confidence Level Index. **Figure 4** derives the formula to obtain Cybersecurity Wellness Index.

Ten Trusted Facilitators (TF) were selected and deployed to interact with 20 Critical Organisation selected with on average two organisations for each TF. The use of TF was important as they were the trusted agent that have the trusting relationship with the respective sampling organisations and have been trained for about one month on how to use the proposed evaluation framework and interpret them correctly for each sampling organisations.

A Trap Case Scenario: The rationale of 50 points deduction is made based on the principle that an organisation that does not keep track of security incidents or breaches is actually blinded of the incoming cyber threats, and therefore can never be effective in protecting its own cybersecurity.

Figure 1 Penalty for having a Trap Case Scenario

Cybersecurity Index = Best Efforts – Annual Cybersecurity Incidents

where:

- Best Efforts = (Total Accumulated Score Points / Maximum Points Possible) x 100
- Annual Cybersecurity Incidents = total number of cybersecurity incidents captured in last annual cycle

Figure 2 Cybersecurity Index

CATEGORY OF CONFIDENCE LEVEL	CONFIDENCE INDEX LEVEL
Internal Evaluation (Voluntary)	One(1)
External Evaluation (Voluntary)	Two (2)
Internal Evaluation (Formal/Regulatory)	Three (3)
External Evaluation (Formal/Regulatory)	Four (4)

Figure 3 Confidence Level Index

$$\text{Cybersecurity Wellness Index} = [\text{Cybersecurity Index} : \text{Confidence Index}]$$

Figure 4 Cybersecurity Wellness Index

4. Business Case Description

4.1 ITU and Estonian Initiatives

The conceptual framework of cyberwellness under the International Telecommunication Union (ITU) initiative considers five key components to be accounted for in its index computation and profiling considerations namely Legal Measures, Technical Measures, Organisational Measures, Capacity Building and Cooperation [3]. We observed that the ITU Global Cybersecurity Index and Cyberwellness Profile Framework and Evaluation data collection process is based on top down hierarchical approach and top-down feedbacks mechanism [3]. Top down approach means data collection methods were executed based on feedbacks and responses of respective top government officials in a hierarchical manner from every ITU member countries. Data collection was focused on building up an information inventory of all ITU member countries based on five core areas mentioned on what has been implemented, initiatives in the pipeline and measures that is yet to be implemented with reasonable supporting evidences to gain the required merit points.

Besides ITU, the other work along this top-down benchmarking perspective is currently being promoted and carried out by the Estonian Government, in which the data collection work is still going on until today. The Estonian project was initiated by the e-Governance Academy in collaboration with its Ministry of Foreign Affairs. The project is called the National Cyber Security Index and was initiated in 2015 [7].

4.2 Definition of Cybersecurity Wellness

In this paper, we will start by introducing and defining cybersecurity wellness, moving away from undefined term of “cyberwellness” used in the ITU-GCI 2015 project. Firstly, we are very interested to use a new term “cybersecurity wellness” due to our interest to the wellness of cybersecurity in Critical Organisation [4] and not only on the generality of cyberwellness even though it may contain cybersecurity as part of its components. In this research paper, cybersecurity wellness is defined as “the state of well-being of all cybersecurity vital signs that can be found in any Critical Organisation (CO)”.

There are many ways to define vital signs. In this research, we are keen to propose compilation of vital signs based on the Annex A of the ISO/IEC 27001 standard [8]. As per the referred Standard, there are currently 114 vital signs which can be extracted from this

Standard and are highly recommended to be monitored by all COs. These vital signs are much easier to handle than the recent NIST Special Publication Draft Document 800-53 Revision 5 which is currently being circulated to industry participants for comments [9]. NIST 800-53 Revision 5 has more than 300 vital signs to go through with and require bigger efforts and higher complexity of tracking them. As our approach to the concept of cybersecurity wellness evaluation is quick, holistic and bottom-up, all these 114 Vital Signs are the rightful choice to be observed by all COs as constant parameters in our wellness index, to ensure accurate response and interpretation consistency in this cybersecurity evaluation framework. The reason for our selection is so fundamental as these 114 Vital Signs have been the gradual improvements of ISO works for many years back in addition to its origin of the British Standard dated back to the year 1995, known as the British Standard 7799 then.

4.3 Our Preferred Approach: A Bottom-Up Perspective

In this research paper, a bottom-up evaluation approach refers to the data collections and feedback methods that are generated based on the cybersecurity performance of all participating organisations collectively using consistently 114 vital signs for each COs evaluated. As we are having 20 participating Critical Organisations for this research, the proposed evaluation framework was applied to all 20 COs and data collections were based on pre-prepared set of questions proposed by the evaluation framework. This collection of 20 participating COs' data were using purposeful sampling [6] of relevant industry or group of organisations operating in critical sectors such as telecommunication industry, power industry, financial industry, etc. done collectively.

As more organisations participating in this research, the database will become larger and resulted into a more accurate representation of the actual situation and can be aggregated upwards to the sectoral and national level, from a bottom-up perspective. This bottom-up approach is the opposite of the ITU and Estonian top-down approach in generating global cybersecurity index and cyberwellness profile, where their data collection methods were relying on feedbacks and responses of top government officials from participating nations as their main source of information. Top-down approach is much simpler to implement from macro-perspective level, but the actual situation on the ground may not be as good as its description from higher level.

Thus, in this research, we were interested in developing a bottom-up approach, the ground level measurement instrument by monitoring and assessing organisation of various types as the smallest unit level to be measured on the ground. The collective results of all cybersecurity vital signs using a bottom-up approach can provide a much more accurate representation and visualisation of cybersecurity wellness and reality at ground level and collectively aggregated upward to make up a bigger view much more accurately. This includes the readiness and effectiveness of implemented security controls and safeguards by all COs within the national jurisdictions. Not only limited to CO, any other type of organisations can also use this proposed Evaluation Framework, to evaluate their cybersecurity wellness status individually and collectively. Collective data of many participating Critical Organisations can form an aggregated cybersecurity wellness index to represent a specific group condition, sectoral or national cybersecurity situation in an empirical manner and provide an alternative view to top-down approaches of cybersecurity performance benchmarking.

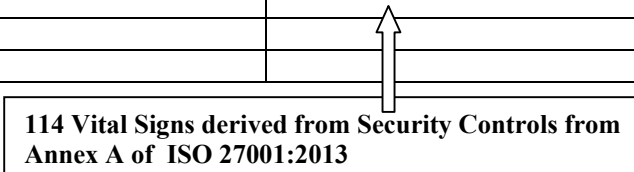
4.4 The Proposed Framework

Our proposed evaluation framework combined the best components of NIST Framework for Improving Critical Infrastructure Cybersecurity [10] and Annex A of the ISO

27001:2013 [8]. The simplest category extracted from NIST framework is Function, Category, Sub-Category. Under Function, the scope is further divided into 5 sub-areas namely Identify, Protect, Detect, Respond, Recover. Under Category, there are 22 Control Objectives, in which selected and appropriate controls can be further divided under subcategory based on the appropriateness of the security controls correlated to each Function and Category [10].

The ISO/IEC 27001:2013 is a well-known standard for information security management system and implemented by many organizations world-wide [8]. In this research the main focus is the Annex A (Normative) of this Standard, Reference Control Objectives and Controls, which listed to our count, one hundred and fourteen (114) controls, excluding Clauses title and Control Objectives. In our proposed framework, we have converted these 114 controls into 114 Vital Signs being used to populate the subcategory column of the combined framework as shown in Figure 1 below.

FUNCTIONS	CATEGORIES	SUBCATEGORIES
Identify		
Protect		
Detect		
Respond		
Recover		



114 Vital Signs derived from Security Controls from Annex A of ISO 27001:2013

Figure 5 Simplified Cybersecurity Framework Derived From NIST and ISO

The Vital Signs Points System was generated by giving points to each of the 114 questions derived from 114 Vital Signs used by the proposed Framework. On each question, the point issued based on a Likert Rating Scale [11] as follows:

- Zero(0) – If the answer is “Not Implemented”, then zero (0) point is attributed.
- One (1) – If the answer is “Need improvements”, then one (1) point is attributed.
- Two (2) – If the answer is “Meeting Expectation”, then two (2) point is attributed.
- Three(3) – If the answer is “Very Effective”, then (3) point is attributed.

4.5 Data Collections Using Semi-Structured Interviews and Focus Group Discussions

Ten groups of Trusted Facilitators were deployed to approach twenty (20) selected Critical Organizations surrounding Windhoek, Namibia. The role of the trusted facilitator is to assist the implementation as to make it as simple and as flexible as possible for the participating organization to respond and to reduce the learning curve. The whole exercise had been completed in less than a day by each facilitator, when the right contact person was interviewed and when all the evidences were made available. These facilitators had introduced the proposed framework and interviewed the person in-charge in these respective critical organizations based on the framework template prepared using an Excel spread sheet as shown in **Figure 6** next page.

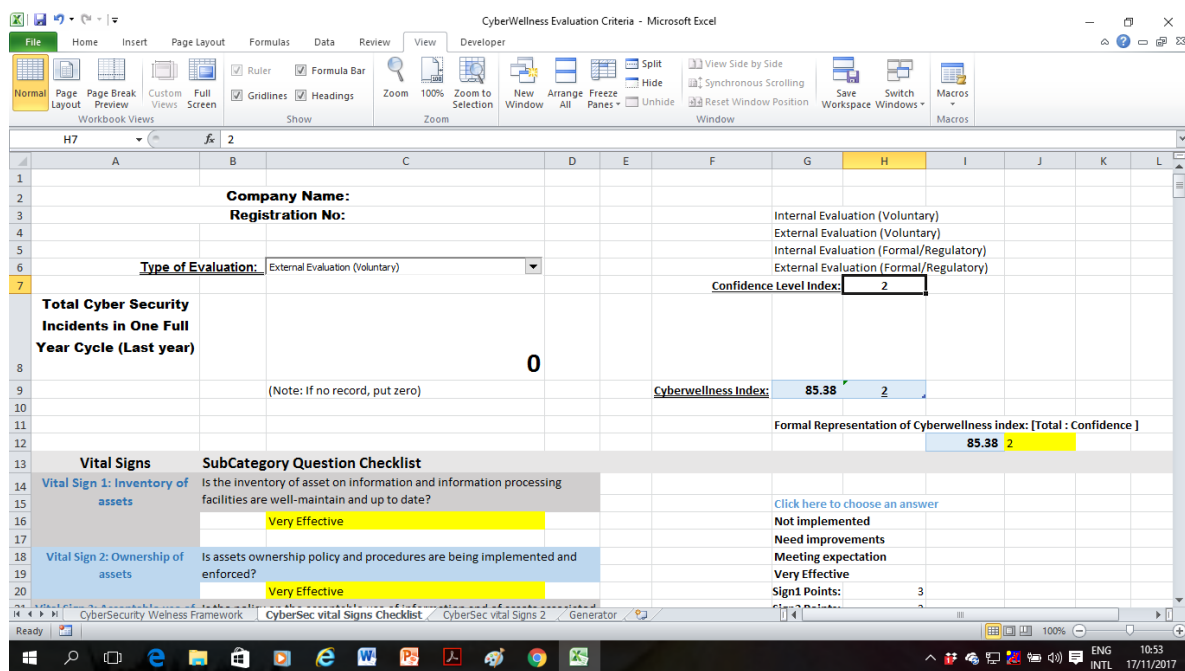


Figure 6 Snapshot of Top Page of the Proposed Framework in the Excel Format

Extraction of relevant results based from completed field experimentations are listed below under **Figure 7** to show some interesting output from randomly selected facilitator's group.

Function	Most Prevalent Level of Risk	% Represented by the most prevalent risk
Identity	High	56
Protect	High	46
Detect	High	78
Respond	High	83
Recover	High	100

Figure 3 – Group 2 Result

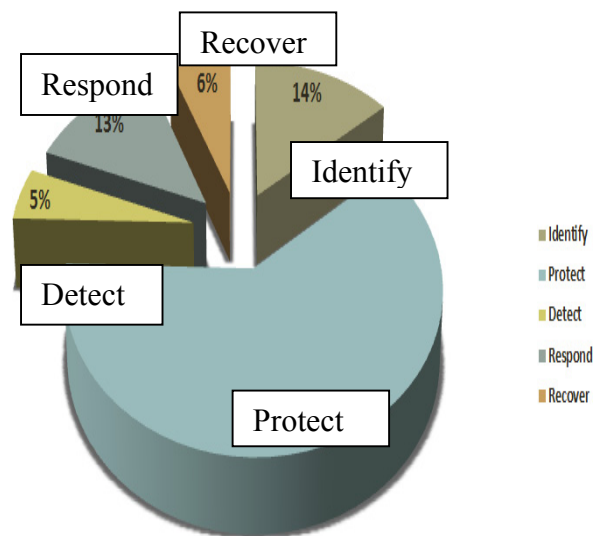


Figure 4 - Group 9 Result

Figure 7 Summary of Cybersecurity Wellness Results Without Index

Figure 8 on the next page shows how data was collected from one organisation using Excel template and given the appropriate marks based on Likert Scale and the accumulated value from 114 cybersecurity vital signs made up the total scorecard that was used for calculating Cybersecurity Wellness Index.

Figure 8 Summary Data of the Namibia University of Science and Technology Cybersecurity Wellness Index – Front Page

The following observations and interpretations were recorded:

- ## 5. Business Benefits

The proposed cybersecurity wellness evaluation framework provides us with a good insight as how to see the actual situation using a bottom-up approach. This framework offers an alternative view to the current top-down approaches that are being practised now by the ITU member countries and those participated in the Estonian project. This framework also offers a practical measurement index based on agreeable cybersecurity vital signs that have

become the practise in many ISO member countries. With this bottom-up approach to cybersecurity wellness evaluation, it provides a good option to many parties to make use of it effectively.

6. Conclusions

Based on this research work, a simpler option to provide an accurate cyber early warning system for Critical Organisations and Critical Infrastructure organisations has been made available. It would be interesting to see if wider adoption to this framework can be done at sectoral level, national level and international level. Making use of cybersecurity wellness index as a tool for comparative analysis makes our understanding of current cybersecurity risks simpler than what it used to be and can be comprehended better by top management and shareholders of these Critical Organisations. This framework provides a simpler way to assess critical organisations from operational perspective, and aggregated up to depict tactical and strategic view as a bottom-up approach to complement top-down evaluation approaches by the ITU Cyberwellness and the Estonian National Cybersecurity Index.

References

1. Global Wellness Institute (GWI). (2016). The History and Facts of Wellness. Retrieved from <https://www.globalwellnessinstitute.org/history-of-wellness/>
2. Bazigos, M. (2015). Fostering Organisation Health and Wellness. *People & Strategy*, Vol. 38 Issue 1, p52-55, Database: Business Premier Source.
3. Jazri, H. 2016. A Quick Cybersecurity Wellness Evaluation Framework for Critical Organisations. IEEE Publication DOI 978-1-5090-5515-9/16/\$31.00 ©2016 IEEE
4. International of Telecommunication Union (ITU-CGI). (2015, April 01). *Global Cybersecurity Index and Wellness Profiles*. Retrieved from <http://www.itu.org>
5. Pasian, B. (2016). *Designs, Methods and Practices for Research of Project Management*. New York. Routledge.
6. Bryman, A. & Bell, E. (2014). *Research Methodology*. South Africa: Oxford University Press.
7. E-Governance Academy (EGA). (2016). *National Cyber Security Index (NCSI)*. Estonia. Retrieved from <http://ncsi.ega.ee>
8. International Standards Organisation (ISO). (2013, October). *ISO/IEC 27001:2013 Information Security Management Standard*. Retrieved from <http://www.iso.org>
9. National Institute of Standard and Technology (NIST). (2017). *Draft NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organisations*. Retrieved from <http://www.nist.gov>
10. National Institute of Standard and Technology (NIST). (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from <http://www.nist.gov>
11. Petrillo, F., Spritzer, A.S., Feitas, C.D.S., Pimenta, M. (2011). Interactive Analysis of Likert Scale Data Using a Multichart Visualization Tool. *Proceedings of the 10th Brazilian Symposium on Human Factors in Computing Systems and the 5th Latin American Conference on Human-Computer Interaction*, Brazilian Computer Society.