From Information Security to Cyber Security Cultures

Organizations to Societies

Rayne Reid
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
s208045820@live.nmmu.ac.za

Johan Van Niekerk
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Johan.VanNiekerk@nmmu.ac.za

***Abstract*—Currently, all Internet and ICT users need basic levels of cyber security awareness and knowledge to perform their daily activities securely. Many security specialists and, indeed, nations are acknowledging the need for populaces to be aware of and educated about being more cyber secure. To achieve cyber security in current populations and to ensure continuity in future populaces, a "self-renewing" belief which affects behavior is needed. In an organizational context this need is met through the fostering of an information security culture (ISC). Similarly, in a societal context a cyber security culture (CSC) ought to be fostered. This raises the question of what precisely would constitute a CSC and how it differs from an ISC. The objective of this paper is to propose ways in which a CSC may be defined and viewed in comparison to an ISC.**

Keywords-information securty culture; cyber security culture; definition; human factor

I. INTRODUCTION

In today's information-centric society the securing of information for information communication technologies (ICT) and ICT users has become of paramount importance. Organizations have long acknowledged this, and have consequently implemented suitable information security solutions. Unfortunately, many of these information security solutions are innately flawed, as the components of such an information security solution and its management involves processes, technology and people [1]. Although processes and technologies can be created to be theoretically secure, how truly secure they are depends on the people involved in their use and implementation [2]. Furthermore, whether people use the technologies in a secure manner and follow the secure processes completely and correctly can drastically affect the extent to which these components are secure, because people can consciously and unconsciously become a threat to any information security solution [3]. As a result of this failing, many authors acknowledge that the people involved are the weakest link in information security [2]–[6].

To counter this human factor, researchers suggest as a solution the fostering or development of a culture of information security [3]–[5], [7]. An information security culture includes all the socio-cultural measures that support technical security methods, so that information security becomes a natural aspect of the daily activity of every employee [8].

Organizations have thus for a while now been fostering an information security culture (ISC) within themselves. These ISCs have been widely accepted as viable counters to "human factor" threats in information security. However, merely fostering such cultures in an organizational context is no longer sufficient to protect the majority of users. Moreover, the need for information security is no longer considered to be solely an organizational issue.

The world beyond organizations has become and continues to be progressively more information-oriented. This means that the average citizen is increasingly being exposed to related risks and threats targeting their transactions, information and own selves. The risk of the average citizen being exposed to the technologies and their associated risks has therefore increased. Consequently, information security principles have become applicable to information use in a personal context. Currently, all Internet and ICT users need basic levels of cyber security awareness and knowledge to perform their daily activities securely.

Security issues relating to the cyber-world require a coordinated and focused effort from national and international society, governments and the private sector. To suit this broader security context a security solution with a greater scope than organizational information security is required. Many security problems primarily exist outside an organizational context, affecting individuals who use the web in a private or social context. Cyber security is thus a solution which focuses on this all-encompassing broader context.

Cyber security is the protection of the interests of a person, society or nation, including their information and non-information-based assets that need protection from the risks relating to their interaction with cyberspace [9]. Humans and their societies are part of the assets needing protection. Many security specialists and nations are now acknowledging the need for populaces to be aware of and educated about being more cyber secure. To achieve this within current populations, and ensure continuity within future populaces, a "self-renewing" belief which affects behavior is needed. In an organizational context this need is met through the fostering of an ISC. Similarly, in a societal context a parallel cyber security culture (CSC) ought to be fostered. This raises the question of what precisely would constitute a CSC, and how does this differ from an ISC.

The objective of this paper is to propose how a CSC may be defined and viewed in comparison to an ISC. This paper

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

will aim to meet this objective by, firstly, demonstrating the need for a cyber-security culture in current society; secondly, examining what known views of information security exist; and thirdly, determining whether cyber security differs from information security. Finally, the paper will conclude by identifying which components and considerations of a CSC will differ from their predecessors.

II. Methodology

This paper presents a comprehensive literature review of sources relating to ISCs and CSCs. ISCs will be the primary focus as limited literature exists. An argument using the review's findings and logical inferences will then be presented to differentiate a CSC from an ISC.

III. Background

The adoption of innovations by society at large is described by the diffusion of innovation theory. This theory explains how, why and at what rate new ideas and technologies spread through cultures [10]. Additionally, it explains the consequences of such diffusion. These consequences can range from positive to negative. To determine whether a particular consequence is positive or not a number of characteristics of the consequence is examined. These characteristics result in the consequence being categorized into one of three categories: desirable versus undesirable (functional or dysfunctional), direct versus indirect (immediate result or result of the immediate result), and anticipated versus unanticipated (recognized and intended or not) [10]. These consequences directly affect the society within which the diffusion of the innovation took place.

In the past the adoption of technological advances, such as the car and airplane, caused major changes to occur within society. These advances had many direct, anticipated and desired consequences. In the case of the car people gained a reliable means of personal travel, they could travel further with fewer inconveniences than before and many business opportunities arose from this. However, these benefits were sadly accompanied by problems. Some of these problems included risks to safety, trade and continued productivity. Car accidents could occur if pedestrians or other cars were not considerate of one another; the conditions of roads affected where people were willing to travel; businesses began to invest more in services that made use of the innovation, rather than those that did not; and finally crimes targeting the technologies came into existence, for example car theft and vandalism. To counter or prevent these risks society had to adapt and accommodate the technology in daily life. Thus indirect and unanticipated consequences of the adoption of the technology included society taking measures such as creating road safety laws; committing to improving and maintaining infrastructure that supported or developed the technologies, for example road maintenance; and the drafting of legislation to account for the crimes relating to the technology. In brief, past technological innovations such as cars have had a major impact on society, changing it forever. Currently, the wide adoption of cyberspace is having a similar impact on society.

The diffusion of cyberspace into society has occurred rapidly over the past few decades. Consequently, many changes have occurred within society to accommodate the Internet as well as ICT. Subsequently, as predicted by the theory of the diffusion of innovations, many positive and negative changes have occurred within society as a consequence.

Cyberspace is an integral part of modern-day society. It is a highly effective tool and enabler of activities. It influences or is integrated (observably and inconspicuously) into all facets of most people's daily lives and digitally transposed activities [11], [12]. Consisting of ICT, cyberspace has become part of the critical infrastructure that supports socioeconomic growth, the governing of nations and sub-societies, the conducting of business and the exercising of human rights and freedom [11]. As part of its desirable and anticipated consequences it has enabled businesses and governments to generate income and employment, provided access to business and information, enable e-learning, and facilitated government activities [11]. As such, the Internet and ICT have become indispensable and have facilitated many positive aspects of the modern way of life. Conversely, however, user adoption of these technologies has also enabled less desirable activities, risks and threats such as information exposure, crime, espionage, terrorism and warfare to make use of these same infrastructure [13].

Subsequently, cyberspace, like technologies such as the car before it, is resulting in a period in which society must adapt to the undesired, indirect and unanticipated consequences of its adoption. In the context of cyberspace and technology adoption, one such consequence which is important for societies is the adoption and use of the measures that have to accompany threats and risks. These most commonly relate to the implementation of information and cyber security. It is unlikely that the adoption of cyber security practices will completely negate the risks posed by such undesired consequences; however, they may greatly mitigate the risks.

A. Information and Cyber Security

Information security is a process involving the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk and maximize return on investments and business opportunities [14]. It involves the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording and destruction [15]. The overall objective of information security is the preservation of the *confidentiality, integrity, and availability* of information and information resources [16]. The protection of these characteristics has become an essential tool in the maintenance of any competitive edge, cash flow, profitability, legal compliance and commercial image to be gained or derived from the ownership of information [14]. Comprehensive information security solutions involve multifaceted physical, procedural and logical forms of protection for the information in question. This type of security is typically implemented in an organizational context [17].

The concept of information security and its relevant practices and procedures is constantly evolving to suit the fluid business environment. However, the mere implementation of

information security solutions by organizations is insufficient [12]. The world outside of organizations has become progressively more information oriented and, as a result, information security principles have become more applicable to information use in a personal context. At present *all Internet and ICT users* need to have at least a basic level of cyber security awareness and knowledge in order to perform their daily activities securely [5], [18]. Security issues therefore now require a more coordinated and focused effort from national and international society, governments and the private sector [19]. This has led to the defining of another type of security, namely, cyber security.

Sharing much of the scope of information security, cyber security principally involves the protection of information and ICT; however, its scope also extends much further [9]. Cyber security involves the preservation of the confidentiality, integrity and availability of information in cyberspace [9]. Cyberspace is a "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" [9]. Therefore, in actuality, cyber security involves the protection of the interests of a person, society or nation, including their information and non-information-based assets that need to be protected from risks relating to their interaction with cyberspace [20]. As the definition of cyber security states, "humans and human societies have grown to become part of the assets that need to be protected" [20]. Therefore, as with information security, humans are still considered to be both a threat and a vulnerability; however, in cyber security they are also considered to be an asset needing protection in cyberspace [9].

Thus information security is the protection of *information*, which is an asset, from possible harm resulting from various threats and vulnerabilities [20]. Comparatively, cyber security is the protection of *cyberspace* itself, as well as the protection of those that *function in cyberspace* and *any of their assets* that can be reached via cyberspace [20].

Traditionally, *organizations* have implemented some form of protection for information resources in the form of information security. However, as the boundaries of information usage moved beyond the organizational context, so too did the associated risks. Subsequently, within this larger *societal* context, based on the previously discussed definitions, the need for *information security* has largely been superseded by the need for *cyber security*.

*ISO/IEC 27032 (*2012) and the previously discussed definitions all indicate that the boundaries of cyber security and the risks it protects against are greater than those of information security. In a societal context (which encompasses organizations and individuals), the risks and threats faced by users are more encompassing than those addressed by typical information security. Therefore, in a societal context it is necessary to look beyond the organizational information security boundaries. The incorporation of cyber security solutions into society is the area of study for this research.

Most previous security-related research dealt with information security, not cyber security. Additionally, the majority of this research was conducted within an academic or organizational context. However, it would be prudent for researchers of cyber security to take heed of lessons learnt from information security, because cyber security still overlaps significantly with information security. The terms "information security" and "cyber security" are also often used interchangeably in the literature. Therefore, although this research focuses on cyber security, of necessity it also examines the literature relating to information security.

B. The Need for a Cyber Security Culture at a Societal Level

Siponen (2001a) states that all users who are involved with any form of ICT or services, particularly in an Internet environment, need to have at least some level of information or cyber security awareness. This statement indicates that users both within and outside organizations need to be cyber security conscious. Subsequently, having organizations as the sole primary practitioners of information security practices and awareness was not deemed sufficient to meet all of these users' needs. Siponen identifies five security dimensions of awareness, and their key issues, that needed to be addressed in order to meet all users' security needs. These dimensions include the organizational, general public, socio-political, computer ethical, and institutional education dimensions [12]. The raising of awareness in all of these dimensions could lead to a cyber security aware culture within an entire society.

The need for cyber security practices and awareness outside of organizations has been further proven over the past decade. In current society, governments in several countries (including the United Kingdom and the United States of America) have recognized the many potential benefits that the adoption of the Internet and ICT may have for their country's welfare [11], [21], [22]. Therefore, in many of these countries citizens are being actively encouraged to adopt these technologies. Unfortunately, although these pro-technological progress movements are having some positive results, they are also having some unintended consequences. One of the most prominent problems is that these societies are establishing a trend of becoming increasingly technology dependent whilst also becoming increasingly vulnerable to cyber threats [23]. This is because many users are not significantly aware of or secured against the cyber threats targeting them via the adopted technologies. This alarming trend needs to be corrected. A potential approach to alter this trend is attempting to foster a culture of security awareness.

Ultimately, entire societies need to be security conscious. Consequently, as part of the socio-political dimension many countries' governments are beginning to recognize that the socio-political and cultural necessity of cyber security awareness is an important factor in the wellbeing of their citizens [12].

Cyber security has become a matter of global interest and importance. Currently, different countries already have different states of security awareness. Increasing their states of security awareness for their national, corporate and citizen safety is unequivocally important for all countries [18]. Thus it is becoming vital that organizational and general users all receive proper security awareness training as soon as possible, in order to reduce the security risks to themselves and to other countries [18]. Already more than fifty nations have officially

published and begun to implement some form of cyber security strategy [11]. Several countries are beginning to implement national cyber security solutions so as to actively encourage their citizens to become cyber security aware. The implementation, maintenance and improvement of these national cyber security solutions comprise a vast range of components, ranging from the operational/administrative level to the tactical [11].

The starting point in each of these efforts is the government showing its commitment to the cause by drafting a national cyber security strategy and other documents of a political nature (laws, regulations, technical and operational protection measures etc.) [11]. Thus the first component of the solution deals with the prescribing of physical, technical and operational controls [9]. However, a true cyber security solution requires more than these controls. This is because the issue of the human factor in security has become increasingly prominent alongside technical issues [24], [25]. Cyber security recognizes the people (human factor) involved with the solution as simultaneously assets, threats and vulnerabilities. It is therefore vital that this component of a cyber security solution is specifically dealt with.

In an organizational context, most current approaches to addressing this human aspect of information security agree that an information security culture should be fostered among users [26]–[28], as this is vital to the success of information systems governance, risk management and compliance [29]. Within the context of a national solution the scope of the human factor would be even greater; however, the solution may be theorised to be similar. Therefore there is a need to foster a culture of cyber security awareness within society.

This raises the following questions: "What constitutes a cyber-security culture?" and "How does it differ from an information security culture?" To begin to address these questions the following sections will firstly examine ISC as a concept and will then identify the way in which a CSC and an ISC would differ.

IV. How a Cyber Security Culture Differs from an Information Security Culture

A. Information Security Culture

Culture is broadly considered to be the overall, taken-for-granted assumptions that a group has learnt throughout history [30]. It emerges over time and is visible in views and actions which reflect a belief [4]. ISCs build on this premise.

Organizations have acknowledged the need for an ISC within a business context. In the past it was found that the technical and procedural components of an information security solution were not in themselves sufficient to address the human aspects of information security [5]. This led to the recommendation that security be embedded in the organization through the institutionalization of information security. Von Solms called this the Third Wave of security [5]. One aspect of this institutionalization of security involved cultivating information security as a corporate culture; that is, information security standardization; international information security certification; the implementation of metrics to continuously and dynamically measure information security aspects in a company; and finally, the *cultivation of an information security culture as a corporate culture* [5]. These recommendations have since been and continue to be implemented, improved and researched.

Many authors have dealt with the topic of ISC ([2][31][4], [32], [33]). Most of these authors focused on cultivating, assessing or auditing a culture. To achieve this, the authors had to explain what they considered an ISC to be comprised of. Literature shows that they commonly based their understanding and representation of an ISC on adaptions of Schein's three-tier organizational culture model [8]. The tiers of Schein's organizational culture model consist of underlying assumptions, espoused values and artifacts [30]. However, this model deals with organizational culture in general, not ISC specifically, and Schlienger and Teufel seldom provide in-depth explanations about how their interpretation of the adapted model translates to the context of information security. This left much about the practice to be subjectively interpreted. Van Niekerk and Von Solms bridged this gap in knowledge by presenting a conceptual model of an ISC which expanded on Schein's model and focused on explaining how the culture's underlying components and processes could influence one another [6].

Van Niekerk and Von Solms's definition of ISC derives from and expands Schein's organizational culture model. Schein lists artifacts, espoused values and knowledge as dimensions of his culture model [30]. Van Niekerk and Von Solms expanded the ISC model by concretely integrating the requisite underlying *information security knowledge* as a separate component in their model [30]. This knowledge dimension was included as the authors theorized that in order to foster an ISC successfully (as a subculture within an organizational culture), all business activities would need to be performed in a secure way [33]. Adequate information security knowledge and skills were therefore deemed a necessary requisite to enable an employee to be able to perform any business activity in a secure manner [6]. Accordingly, their conceptualization (as shown in Fig. 1) of an ISC consists of four information security-related components, namely, artifacts, espoused values, shared tacit assumptions and knowledge [6].

The exact contents of each of the other dimensions were also slightly altered in order to be more context-specific to ISC. The ISC-specific interpretation of the model dimensions therefore now refer to the following framework components:

1. *Artefacts (AF)* – Detailed procedure of the organization's daily tasks. This dimension includes the visible structures and processes which were deemed to be "measurable but hard to decipher" [6]. Examples of these would be the architecture and security mechanisms of the company, as well as information security policies and procedures.
2. *Espoused Values (EV)* – The guidelines for what to include in a policy, and subsequent ISC to adequately address the business's needs. These include information security strategies, goals and philosophies. In brief, the information security-related espoused justifications and official viewpoints [6].

3. *Shared Tacit Assumptions (STA)* – The beliefs and values of the individual and collective employees. This includes their unconscious, taken-for-granted beliefs, perceptions, thoughts and feelings. In brief, it is the layer at which the people are involved and as such it is the ultimate source of values and action [6].
4. *Knowledge (KW)* – The necessary and required levels of information security-specific knowledge needed to perform the daily business tasks in a secure manner [6].

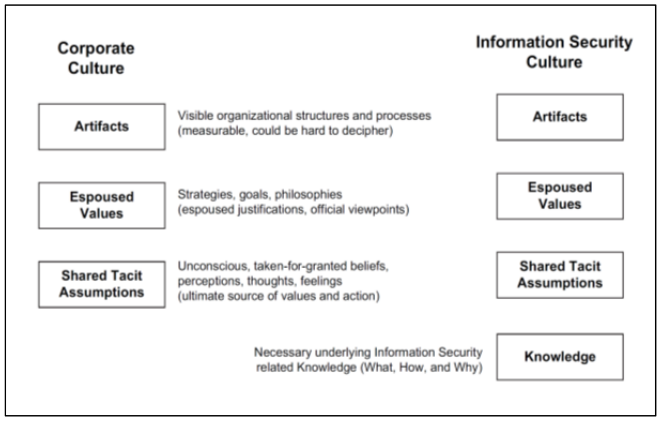

Figure 1: Levels of culture. Adapted from Schein (1999, p. 16) [6].

This adaption of Schein's organizational culture was very suitable for an ISC. This is because thus far the literature has dealt with ISCs that were cultivated, assessed, audited and so forth in an *organizational context*.

However, in terms of this CSC research, the use of Schein's model may be questioned and requires further justification. Schein's model depends on its organizational context and an understanding of how a culture can be cultivated or measured within this insulated environment. The previous section has shown that cyber security extends beyond the contextual borders of an organization. This extension of scope will likewise affect the CSC. Therefore one should ask whether Schein's model is acceptable for use with a CSC, or would other models such as the one offered by Hofstede [34] be more suitable. The next section will examine these considerations as well as others for a CSC.

B. Considerations for a Cyber Security Culture

All of these previously mentioned ISC models focused on an ISC in organizations. This paper aims to address the ISC needs of a society. The previous sections established that a CSC will likely be similar to an ISC; however, there will be some definite differences. This section will examine some of the differences that exist and the considerations that have to be made. The issues that will primarily be discussed relate either to the CSC's context or its components.

1) Context

The first significant difference between an ISC and a CSC would, as the previous section noted, be the context in which the culture would be fostered. Information security cultures are cultivated and managed within insulated organizational contexts. This context translates to being a relatively well-controlled environment with relatively predictable user behavior, activity and profile sets. Comparatively, with the scope of a cyber-security solution the culture would be cultivated within a societal scope. The environment within a societal context would likely be less controlled; user profiles would range across many skillsets, age ranges and other variables; and the activities being performed by the users would be less predictable than those within a purpose-based organization.

These differences would affect the ease with which a culture could be established and the degree to which the users may be willing to subscribe to the culture. It is probable that attempts to foster an ISC may experience faster and more complete success than attempts the foster a CSC in society. This is because organizations tend to have a number of cultures or behavior sets which they seek to instill within their employees. It is possible that employee exposure to a number of such continuous culture fostering processes with a particular (arguably regulated) environment may make them more amendable to accepting other cultures in the same environment. Comparatively, a societal context is less closely regulated. For example there are broad-based culture systems, such as national culture, religious culture etc. and even smaller community cultures, which are less regulated than those within a work environment. Therefore the users are more likely to be individualistic than when they are in their work environment.

Within the context of an ISC, Furnell and Thomson identified a number of factors that could be theorized as affecting the users' (involved in a solution) willingness to comply with the culture [2]. These factors may also affect whether a societal user would be willing to accept a cyber security culture. The factors which should be considered for the CSC are the following: the roles the user must play; the nature of the task; user behavior and the psychology of the users [2]. How the various elements of an ISC and a CSC will differ will now be briefly discussed.

The role, current task and user behavior that the users must adopt from a security perspective while completing their tasks would relate to who they are and what they are doing [2]. Within the context of an ISC this role would relate to what the users are actually expected to do as part of their job, and their security responsibilities required by the job. Within this context the role should be easily defined, as a user will be goal/task oriented to the organization's work process. Therefore, a user will only be expected to consider their role and responsibilities for their part of the task. They would not be expected to know how to fulfill the roles outside their own job description. For this user the number of roles they may play will thus be limited and they will only need to adopt the culture pertaining to these limited roles. In comparison, in a personal capacity within a societal CSC, the number of roles a user may play will be dependent on the activities they as an individual elect to complete. The user may have some fixed tasks as well as many ad hoc tasks which have varying contexts. This means that a user within a CSC would need to be exposed to a broad culture which shows them how to adapt their roles based on a task. This factor also relates to the

general user profiles involved in the culture. Within an organization, certain age ranges, skillsets and suchlike are expected and thus their roles relate to these characteristics. However, when in open society the types of role characteristics are infinitely combinable.

Having now determined how the contextual considerations that will affect the consideration of a CSC, the next subsection will establish how the components of the cultures will differ.

2) Components

As a result of the comprehensiveness of Van Niekerk and Von Solms's definition of an ISC [6], the focus on the conceptualization of an ISC and the degree of similarity of the degree relative to the explanation to a CSC as well as the ISC, this paper will adopt their definition of an ISC to discuss the similar aspects of a societal CSC.

As discussed in the previous section, Van Niekerk and Von Solms conceptualized an ISC as having four component levels, namely, Artifacts (AF); Shared Tacit Assumptions (STA); Espoused Values (EV) and requisite information security Knowledge (KW). In the context of a CSC it is likely that similar abstract components would also exist. However, how they translate within real-world applications as artifacts and behaviors will differ due to the scope of the context. This section will briefly examine how these cultural components could emerge differently.

The first component to consider would be the EV. Typically, within an ISC the EV describe the values that an organization is said to be advocating or promoting [35]. In the context of an ISC, these EV would be issued by the board of directors or the high-level management on the business's behalf. They would manifest in the business's information security policy, and the business's general vision. This is in an organizational context, but within a CSC the approach would be similar. In terms of the overall societal scope a similar top-down approach would also be necessary; however, the degree to which they may be heeded would likely be more dependent on the context and the users involved than it would within an organization. In the broader society, the espoused values would likely be issued by governmental, national or international agencies and would then manifest as a national cyber security culture. This would be similar to what occurs in the ISC. However, how a CSC may differ in EV is that, in societies, there are a number of sub-societies. And in these sub-societies, there may also be additional author representatives (i.e. top management), which may further issue other EV. These EV would build on the higher level specifications but may not contradict them. Essentially, the EV in a CSC would be notices such as rights, laws and national policies. Therefore they would cover very broad areas.

The second component to be considered would be the artifacts (AV). This component strongly relates to the espoused values. Considerations for this component are the following: Artifacts are the observed concrete or tangible behavior, or what an individual can see, hear and feel when they observe an organization. [35]. Therefore, in an ISC, examples of these would include the physical security, the information security policies and the procedures. In an organizational context these artifacts are capable of being very specific in their requirements. Comparatively, however, the artifacts of a societal CSC would likely involve national policy, laws and other recommended best practices. Owing to the nature of these potential artifacts, they would not be as easily established, or created to be as specifically detailed as an organization's artifacts. This raises the question of how to communicate the more specific recommendations to the users in society.

The next consideration are the Shared Tacit Assumptions (STA) that are shared by a group of people and encompass the underlying thoughts and values that the employees of an organization believe to be true [35]. This level of corporate culture directly influences the behavior of employees that can be observed at the artifact level. In terms of an ISC versus a CSC, this level will be more easily measured or perceived in an organizational context. The STA among users in a society will exist; however, because users will also belong to sub-societies, they will develop individualized instances of STA. Therefore, in a CSC these STA will be more difficult to observe. Determining what STA exist will therefore be more difficult in a CSC.

Finally, the knowledge component will have to be considered. This relates to awareness of the requisite security knowledge needed to fulfill the user's security roles while they are completing a task. In both an organizational and societal context the users cannot be expected to have such default knowledge. Therefore this component raises the question of how to provide the users with access to methods to gain this knowledge. Within an organization education and training is part of fostering an ISC. Education would likely also be used in fostering a CSC. However, what content should be included must be determined for the CSC, as the number of activities a user may need to perform securely is not as predictable as it would be in an organizational context.

This section discussed the primary/major considerations that would differentiate a CSC from an ISC. It was established that the components and implementation of a CSC within a societal context would significantly differ from the components of an ISC, although they would serve a similar purpose. It is the authors' belief that the CSC and the ISC are very similar; that the broader context of the CSC would have a major effect on the way a CSC is fostered in society compared to the way an ISC is fostered in an insulated organizational context. This theory will have to form part of future work.

V. CONCLUSION

The world's rapid adoption of cyber technologies and services has exposed users to the many beneficial services and conveniences offered by the cyber world. However, it has also exposed them to many threats. Exposure to increasing threats and potential risks has led to cyber security knowledge and skills becoming a vital life skill for all cyber citizens. Therefore, as an important life skill they should be integrated into citizens' daily cyber behavior to the extent that it becomes an unconscious action. A CSC should thus be fostered.

The literature has shown that many studies have been conducted and frameworks or guidelines for the fostering of

information security cultures proposed. These cultures are, however, confined to the organization's environment and similar-sized insulated (controlled) environments. Nevertheless, compared to ISC, there are no widely accepted definitions or guidelines for what constitutes a CSC. To begin addressing this gap, this paper has proposed a conceptual understanding of the probable components and the consideration of a cyber security culture. Although the discussion presented here is not a definition of CSC, it does identify the questions, components and considerations that should be taken into account when defining a CSC. One of the major considerations for a CSC would be its lack of an insulated overall environment, because societal boundaries are considerably broader than the organizational boundaries of an ISC. It is therefore the recommendation of this paper that cyber security not be defended as an abstract concept to be applied to all contexts. Rather is it is recommended that CSC should be defined to suit particular contexts.

VI. Future Work

Forthcoming research will examine how to foster a CSC in various contexts.

References

[1] M. Alnatheer and K. Nelson, "A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context," in *7th Australian Information Security Management Conference*, 2009, no. December, pp. 1–3.

[2] S. Furnell and K.-L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," *Comput. Fraud Secur.*, vol. 2009, no. 2, pp. 5–10, Feb. 2009.

[3] K. Thomson, R. Von Solms, and L. Louw, "Cultivating an organizational information security culture," *Comput. Fraud Secur.*, no. 10, pp. 7–11, 2006.

[4] T. Schlienger and S. Teufel, "Information Security Culture - The Socio-Cultural Dimension in Information Security Management," in *Security in the information society: visions and perspectives. IFIP TC11 International Conference on Information Security (Sec2002)*, 2002, pp. 191–201.

[5] S. . Von Solms, "Information security—the third wave?," *Comput. Secur.*, vol. 19, no. 7, pp. 615–620, 2000.

[6] J. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, Jun. 2010.

[7] J. Van Niekerk and R. Von Solms, "An holistic framework for the fostering of an information security sub-culture in organizations," in *4th Annual ISSA Conference South Africa*, 2005.

[8] T. Schlienger and S. Teufel, "Information Security Culture – From Analysis to Change," *South African Comput. J.*, vol. 21, pp. 46–52, 2003.

[9] *ISO/IEC 27032*. Information technology — Security techniques — Guidelines for cybersecurity, 2012.

[10] E. M. Rogers, *Diffusion of innovations*, 5th Editio. New York: Free Press, 2003.

[11] A. Klimburg, Ed., *National Cyber Security Framework Manual*. NATO CCD COE Publicaions, 2012.

[12] M. Siponen, "Five dimensions of information security awareness," *ACM SIGCAS Comput. Soc.*, vol. 31, no. 2, pp. 24–29, Jun. 2001.

[13] M. Siponen, "Towards maturity of information security maturity criteria : six lessons learned from software maturity," pp. 210–224, 2001.

[14] *ISO/IEC 27002*. Organization International Standards, 2008.

[15] J. H. Allen, "The CERT guide to system and network security practices," in *NCISSE 2001: 5th National Colloquium for Information Systems Security Education*, 2001, pp. 1–11.

[16] C. P. Pfleeger, *Security in Computing*, 2nd ed. Englewood Cliffs, NJ: Prentice Hall International, 1997.

[17] R.-M. Ahlfeldt, P. Spagnoletti, and G. Sindre, "Improving the Information Security Model by using TFI," *IFIP Int. Fed. Inf. Process.*, vol. 232, pp. 73–84, 2007.

[18] C. C. Chen, B. D. Medlin, and R. S. Shaw, "A cross-cultural investigation of situational information security awareness programs," *Inf. Manag. Comput. Secur.*, vol. 16, no. 4, pp. 360–376, 2008.

[19] M. Dlamini, "Information security: The moving target," *Comput. Secur.*, vol. 28, no. 3–4, pp. 1–10, 2009.

[20] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013.

[21] "The UK Cyber Security Strategy," no. November. Cabinet Office, 2011.

[22] White House, "The National Strategy to Secure Cyberspace." pp. 1–60, 2003.

[23] S. Furnell, P. Bryant, and A. Phippen, "Assessing the security perceptions of personal Internet users," *Comput. Secur.*, vol. 26, no. 5, pp. 410–417, Aug. 2007.

[24] M. B. Desman, "The Ten Commandments of Information Security Awareness Training," *Inf. Syst. Secur.*, vol. 11, no. 6, pp. 39–44, Jan. 2003.

[25] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the human element of security*. Wiley Publishing Inc, 2002.

[26] J. Van Niekerk, "Fostering Information Security Culture Through Integrating Theory and Technology," Nelson Mandela Metropolitan University, 2010.

[27] A. Cox, S. Connolly, and J. Currall, "Raising information security awareness in the academic setting," *Vine 123*, vol. 31, no. 2, pp. 11–16, 2001.

[28] G. Dhillon, "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns," *Comput. Secur.*, vol. 20, no. 2, pp. 165–172, 2001.

[29] S. Dojkovski, S. Lichtenstein, and M. J. Warren, "Enabling information security culture: influences and challenges for Australian SMEs," in *21st Australasian Conference on Information Systems*, 2010, p. 61.

[30] E. H. Schein, *The corporate culture survival guide*. San Francisco, California: Jossey-Bass Publishers, 2009.

[31] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Comput. Secur.*, vol. 23, no. 3, pp. 191–198, May 2004.

[32] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, Mar. 2010.

[33] J. Van Niekerk and R. Von Solms, "Understanding information security culture: A conceptual framework," in *Information Security South Africa (ISSA), Johannesburg, South Africa*, 2006, pp. 1–10.

[34] G. Hofstede, H. G. Jan, and M. Minkov, *Cultures and organizations: Software of the mind:intercultural coopration and is impotance for survival*, 3rd Editio. McGraw Hill, 2010.

[35] S. Furnell and K.-L. Thomson, "Recognising and addressing 'security fatigue,'" *Comput. Fraud Secur.*, vol. 2009, no. 11, pp. 7–11, Nov. 2009.