A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument

Dr Adéle Da Veiga
College of Science, Engineering and Technology, School of Computing,
University of South Africa,
dveiga@unisa.ac.za

***Abstract*—A cybersecurity culture must be promoted at an international, national, organizational, and individual level to aid in minimizing risks from a human perspective in cyberspace. To promote such a culture it has to be understood and quantified in order to direct change. This research makes use of the disciplines of information technology and industrial psychology to define a cybersecurity culture. A quantitative research methodology, cybersecurity culture research methodology (CSeCRM), is proposed that can be used to measure a cybersecurity culture. The objective of CSeCRM is to ensure that a reliable and valid measuring instrument is used to measure cybersecurity culture. The results derived from using such an instrument can aid in identifying actions to change and direct the cybersecurity culture at, for instance, schools or businesses, at national or international level. The CSeCRM is illustrated by implementing it in an organization where a cybersecurity culture measuring instrument was validated.**

Keywords—cybersecurity; cybersecurity culture; industrial psychology; measurement; measuring instrument; quantitative; research methods; statistical analysis; research approach; research methodology; research philosophy

I. INTRODUCTION

It is predicted that by 2020 there will be 50 billion internet-connected devices, including fixed communications, mobile communications, computers, consumer electronic devices and medical devices, industrial devices, and automotive devices [42]. The "internet of things" is bringing about a worldwide culture where citizens are entwined in a digital world. This digital world of interconnected networks and devices can also be described as cyberspace. Cyberspace is defined as "[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers" [28].

While cyberspace brings advantages to citizens, business and governments, it also introduces risk from a security and privacy perspective. Personal, identifiable information (e.g. information on health and children) can be exposed, unauthorized access can be gained to online banking accounts, an organization's intellectual property can be stolen, industrial devices and machines can malfunction, and networks can be disrupted, to mention but a few risks. Cyber risks can lead to financial loss, reputational damage, and even the violation of human rights because of ignorance on the part of the user or organization, or as a result of targeted cybercrime.

Cybercrime is organized computer crime within the context of cyberspace [41]. It is also defined as the actions of a person (including the utilization of a device or computer program) who intentionally accesses, intercepts or interferes with data represented in any electronic form without authorization [14]. As such, cybercrime can be summarized as the unauthorized access, interception or interference of data within the context of cyberspace, constituting a crime or harm.

Cyber attacks are caused firstly by cybercriminals, then by nonmalicious insiders and thirdly by hackers [26]. The Information Security Breaches Survey [25] confirmed that the human factor is an increasing concern, with three-quarters of large organizations and a third of small organizations experiencing an employee-related breach. Fifty percent of the participants in this survey indicated that the single worst breach suffered in the organization was related to human error. The cyber attacks experienced by organizations vary between internet attacks, customer impersonation, denial of service attacks, organization impersonation (for example, phishing attacks), and actual network penetration [25]. A survey conducted by McAfee and SAIC [37] reported similar findings in that organizations indicated that the most significant threat related to data leaked accidentally or intentionally by employees. They argue that "employees' adherence (or lack thereof) to security procedures is considered to be the greatest challenge to organizations" [37]. The United States Homeland Security published a roadmap for cybersecurity research in which they identify insider threats as one of the eleven critical concerns for research and development agendas of the future [22].

Cyber users pose a risk to themselves and others if they are not educated or do not know how to use cyberspace responsibly and ethically. It has been found that at least 30% of the loss of confidential information in the context of cybersecurity can be attributed to human error and negligence [42], indicating that the human element is an issue that needs to be dealt with from a national and social, but also an organizational perspective. To mitigate cyber risks and minimize cybercrime, cybersecurity is aimed at protecting information resources connected in cyberspace, the information

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

available via cyberspace, and the individual who could fall prey to cyber attacks [52]. Luiijf and Besseling [34] conducted a comprehensive review of 19 nations' national cybersecurity strategies. In this review, they compared the definitions of cybersecurity and found that there is no common or harmonized cybersecurity definition. They argue that the definition of Rauscher and Yashenko [45] could suffice as a definition of cybersecurity as a common understanding of the various nations' definitions. In terms of this definition, cybersecurity is the response and recovery to intentional and unintentional threats in cyberspace. Cybersecurity can therefore be understood as the minimization, mitigation, and response to intentional and unintentional threats in cyberspace in order to protect information resources and humans.

The 19 national cybersecurity strategies are all formulated to reach objectives that can contribute to cybersecurity [34]. In South Africa, the Department of Justice and Constitutional Development published a draft Cybercrimes and Cybersecurity Bill towards the end of 2015 [7] in an attempt to legislate some of the objectives of their national cybersecurity strategy. This comprehensive Bill aims to establish structures such as an integrated cybersecurity legal framework for the country. Among other aspects, the Bill outlines cybercrime offenses (e.g. unlawful access or interference, fraud, terrorist activity, and espionage), defines the concept of jurisdiction, outlines the powers to investigate, search and access or seize with international cooperation, imposes obligations on electronic communication service providers, includes the identification of national critical information infrastructure protection, and includes regulations on aspects relating to evidence.

Having a national cybersecurity strategy and cybersecurity legislation is only part of the solution to deal with cybercrime. The Working Party on Information Security and Privacy of the Organisation for Economic Co-operation and Development (OECD) published a document outlining the efforts of governments in 18 OECD member countries to foster a culture of security [39, 40]. All these countries finalized a national strategy to foster a culture of security to combat cybercrime as one of four key priority areas.

However, the OECD report found as a limitation that the countries spent less time on developing metrics and benchmarks to measure the effectiveness of their national policies to develop a culture of security.

It would be beneficial to understand the culture of, for instance, nations, citizens, employees or children when they interact with cyberspace, in an attempt to minimize the risk that they pose to themselves and others. If the culture of cybersecurity could be measured and quantified, strategies and programs could be developed to direct the culture in order to assist in promoting a safe cyberspace. If aspects of change could be identified to aid users in protecting themselves and others from cyber risks, this may help in dealing with the risk of the human element in cyberspace.

In addition, the cybersecurity culture of an organization can provide insight into the security risk exposure of that organization by including the results as part of an audit of the current information security risk for the purposes of, for instance, negotiating lower premiums for insurance against cyber risk [16]. From a security risk perspective, the assessment of an information security culture can be incorporated in security risk frameworks such as those proposed by Shameli-Sendi, Aghababaei-Barzegar and Cheriet [48] to manage risk from a network infrastructure as well as an employee behavior perspective. The information security culture status in an organization can furthermore also give insight into decision-making from a human perspective in cyber incident management, which could be integrated into the incident response decision frameworks of, for example, He, Maglaras, Janicke, and Jones [19].

This research paper aims to define what a cybersecurity culture is by considering the discipline of industrial psychology and leveraging off the definition of an information security culture, which is discussed in section III. In section IV, a research philosophy and approach are proposed for assessing a cybersecurity culture. A quantitative research methodology, called a cybersecurity culture research methodology (CSeCRM), is proposed in section V to aid researchers in following a structured and comprehensive research process whereby a cybersecurity culture measuring instrument can be validated. The application of the methodology to derive such a measuring instrument is discussed in section V. The paper concludes in section VI with limitations and suggested future research.

II. Research Objective and Questions

The first objective of this research is to define cybersecurity culture in order to arrive at a definition that can inform the measurement of such a culture. A second objective is to identify an appropriate research approach and methodology as a point of reference for researchers when aiming to develop a reliable and valid measuring instrument for a cybersecurity culture. The following research questions are answered in this research:

- What is a cybersecurity culture?
- What research philosophy and approach can be followed to measure a cybersecurity culture?
- What research methodology can be followed to ensure a valid and reliable cybersecurity culture measuring instrument?

The remainder of the paper aims to deal with the research objectives and to answer the research questions.

III. Defining Cybersecurity Culture

To define cybersecurity culture, the definition of organizational culture can be used. Probably the best-known definition of organizational culture is “the way things are done here” [35]. It can be seen as the personality of the organization [46] and the social glue that binds the members of an organization together [32].

An organizational culture develops on the basis of certain activities in the organization, such as the vision of management and the behavior that employees exhibit as individuals, in a group and at organizational level [20, 46]. The organizational culture that develops on the basis of exhibited behavior is evident in artifacts (using encryption), values (“the privacy of

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

customer data is respected"), and basic assumptions ("executive management understand the risk to information") [49].

According to Robbins [46], organizational behavior is about what people do in an organization and about how their behavior affects the performance of the organization. The term also incorporates employee attitude and how it relates to employee behavior in the organization [20].

In turn, an information security culture has been defined as the attitudes, assumptions, beliefs, values, and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior (i.e. incidents) evident in artifacts and creations that become part of the way things are done in an organization to protect its information assets. This information security culture changes over time [8].

From a cybersecurity culture perspective, the organizational environment has to be extended to a national and even international context, including the global connectivity of the internet and numerous technology devices. Cybersecurity culture can therefore be viewed at different levels, from the top downwards (see figure 1), starting with the international cybersecurity culture which includes all devices and people that are connected globally. The security and resilience of a country's critical infrastructure are enhanced by the national cybersecurity culture "to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" [38].

From an organizational perspective, the organization's critical infrastructure and information have to be managed and protected in such a manner that cyber risk (e.g. loss of organizational data via network attacks) is minimized while profits are maximized.

From an individual perspective, if a user utilizes cyberspace, all of the user's assets (e.g. devices, household equipment) that can be connected to cyberspace [52] and the user's personal information shared in cyberspace have to be protected. In all of these areas, a cybersecurity culture is necessary where users interact with cyberspace in such a manner that their behavior contributes to the confidentiality, integrity, availability, and privacy of information and information assets of all parties involved.

However, in order to minimize cyber risk at national, organizational or individual level, controls have to be implemented. Although technology solutions are available, the human factor remains a concern [10, 25, 26, 30].

The manner in which employees (or citizens) utilize cyberspace can introduce risk to themselves, other individuals, organizations or even the country. It is therefore critical that the attitudes, assumptions, beliefs, values, and knowledge of cyber users promote "efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, quality, and civil liberties" when using cyberspace [38].

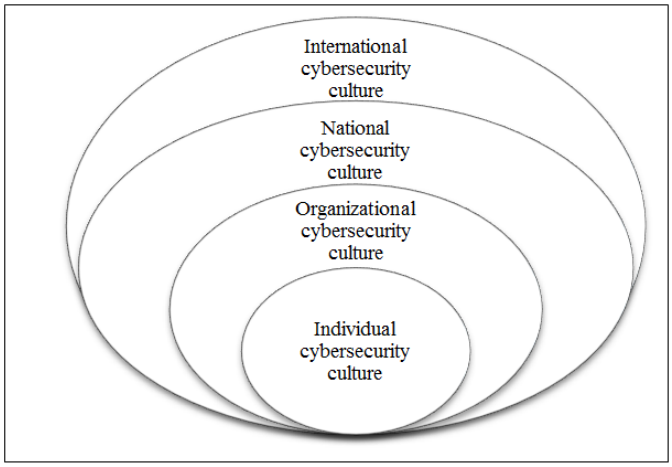

Fig. 1. Cybersecurity culture levels

For the purpose of this research, a cybersecurity culture can be defined as the intentional and unintentional manner in which cyberspace is utilized from an international, national, organizational or individual perspective in the context of the attitudes, assumptions, beliefs, values, and knowledge of the cyber user. The cybersecurity culture that emerges becomes the way things are done when interacting in cyberspace and it can either promote or inhibit the safety, security, privacy, and civil liberties of individuals, organizations or governments.

A measurement of a cybersecurity culture is needed in order to change or direct such a culture of different population groups, for instance children at a specific school, employees of a company, or citizens in a certain region. This will aid in identifying the concepts of cybersecurity ("what") and "how" to educate communities in order to foster a cybersecurity culture that upholds ethical, security, and privacy principles. The next section outlines the disciplines that can be used to research cybersecurity culture and, ultimately, to measure it to institute change at various levels.

IV. Research Philosophy of and Approach to Cybersecurity Culture Research

A. Research disciplines

Two main academic disciplines, namely information technology and industrial psychology, can be used to illustrate what aspects should be considered when conducting cybersecurity culture research. These disciplines were researched as part of an academic dissertation for a doctoral degree in information technology (IT) [8], which focused on information security culture. This was adapted in this research for cybersecurity culture.

- *The discipline of IT*: IT is concerned with the use of technology, which is a combination of hardware, software, telecommunication systems, and other devices to manage and process information for various purposes [17, 51]. These purposes include communication, storage, calculations, meeting business objectives, performing tasks, and automation, to mention but a few. IT is used as the tool or enabler to process the

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

information or data required to achieve the various purposes of individuals, businesses and governments. However, the data and information must be processed in a reliable, accurate, and secure manner. As such, information security is concerned with protecting the information in the IT environment by ensuring the confidentiality, integrity, and availability of the information through the implementation of various controls extending to people, process, and technology solutions [27].

The focus of cybersecurity is to protect the IT infrastructure (hardware, software, and networks), the information, and people [52] using IT in the context of cyberspace, i.e. the internet and connection of various IT devices over a network [44]. According to Baltzan [1], "information technology in and of itself is not useful unless people know how to use and manage it effectively". The human element (e.g. employees, citizens) in interacting with information in cyberspace relates to the human sciences and culminates in industrial psychology.

- *The discipline of industrial psychology*: Industrial psychology is the study of human behavior at work [23]. It is used in the context of this research paper to understand organizational culture and human (e.g. employee) behavior and to assess these elements in, for instance, an organization or at national level. Attitudes and perceptions are examined to understand how a cybersecurity culture develops and how it may be assessed. The methods applied in industrial psychology can be used to understand how to integrate cybersecurity and organizational culture in order to be able to ultimately propose a research approach and methodology for investigating cybersecurity culture.

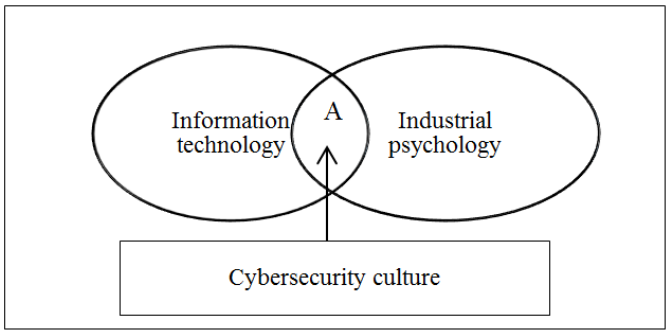

Fig. 2. Research fields for cyber security culture

Figure 2 outlines the two disciplines that were considered in this research for investigating cybersecurity culture. When researching cybersecurity culture, concepts from an IT perspective must be considered, such as cybersecurity, risks, and controls. Cultural and human behavior aspects must be considered from the industrial psychology perspective and specifically from approaches that can be applied to measure and develop or change a culture. As such, cybersecurity culture is depicted in circle "A", indicating that there is a relationship between the two disciplines when researching cybersecurity culture.

B. *Research philosophy of and approach to cybersecurity culture*

The proposed research philosophy of and approach to cybersecurity culture, as adapted from the research onion of Saunders, Lewis, and Thornhill [47], is outlined in figure 3. It depicts six layers, which are embedded in a quantitative approach. The six layers are as follows:

- *Philosophy*: In order to measure cybersecurity culture, a positivism philosophy may be used where a structured methodology is recommended for researching cybersecurity culture using quantitative methods including statistical analysis [47]. According to De Villiers [11], the objective of positivist research is to obtain research results that are reliable, consistent, unbiased, and replicable through other research studies in order to represent reality. However, if focus groups and interviews are used as part of a mixed method to assess cybersecurity culture, one could argue that the philosophy is extending to an interpretivist epistemological orientation whereby some of the critique on quantitative methods can be dealt with, such as the reliance on instruments which could hinder the connection between everyday life and research; and to distinguish people and social institutions from the natural world [5]. In the context of a cybersecurity culture, one might argue that although a survey gives precise and accurate measures of the perceived culture, the survey questions might not be interpreted in the same manner by all employees, nor would employees have the same background of cybersecurity controls when answering the questions. Focus groups and interviews can aid in obtaining more in-depth information on certain variables that are measured using a cybersecurity culture questionnaire. However, a positivist philosophy, using a quantitative method, is primarily proposed for this research in order to propose a methodology to derive a valid and reliable measuring instrument.
- *Method*: A deductive method is often linked with a survey. The research starts with theory and then a hypothesis is deduced from the theory and tested [5]. In the case of a cybersecurity culture, a cybersecurity culture measuring instrument can be used to test certain hypotheses. For example, "IT employees have a stronger cybersecurity culture than operational employees", or "Employees who have been exposed to cybersecurity training will have a stronger cybersecurity culture". If focus groups or interviews are conducted, the method could extend to an inductive method.

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

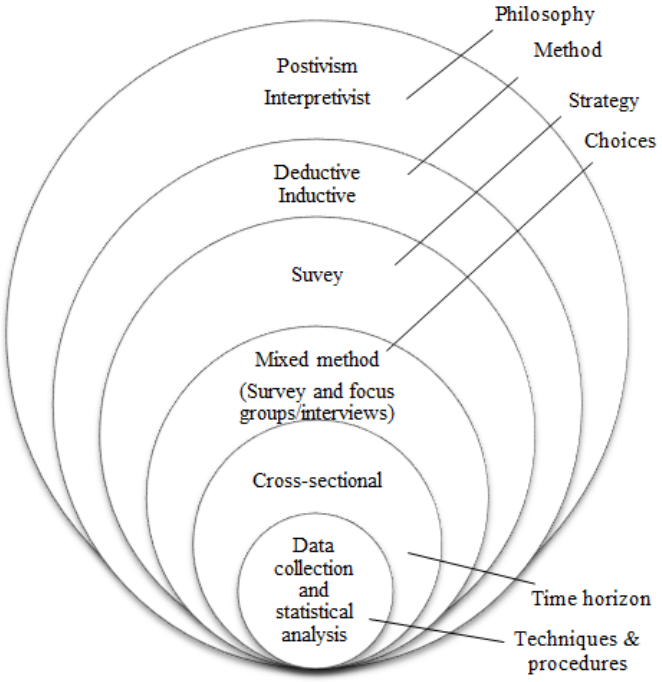

Fig. 3. Cyber security culture research philosophy and approach

- *Strategy*: Quantitative research methods have been used with great success in the information security discipline [2, 29, 50]. One of the benefits of using a quantitative approach is that specific areas of concern (e.g. cyber bullying) among a particular group of people (e.g. school children) and with regard to a specific topic (i.e. cybersecurity culture) can be determined [31]. Questionnaires and surveys have been used widely as research tools in the social sciences [4]. This method is beneficial in descriptive or explanatory research [47]. Surveys are specifically attractive, as they cost relatively little and a potentially large sample of users can participate with minimal resource requirements [4]. Surveys are traditionally used to measure behavioral content pertaining to attitude and opinions [3] by systematically gathering data from the sample population for a specific purpose [31]. To assess the cybersecurity culture, the attitude and opinions of users regarding the use of cyberspace and security controls and practices can be determined. Through such an analysis, citizens or employees' perceptions of cybersecurity can be assessed and aspects identified that require attention in order to improve the cybersecurity culture to an acceptable level, thereby protecting information, information assets, and people.

- *Choices*: A mixed method can be employed to assess a cybersecurity culture. In this case, a questionnaire would be used to perform the quantitative assessment and interviews would be conducted or focus groups formed, as a qualitative technique, to confirm and correct the quantitative data [5]. This can be used successfully when survey responses of, for instance, a specific business unit or area are not sufficient to generalize the findings across the group in line with the sampling requirements. Employees can, for instance, complete questionnaires, followed by interviews conducted with the most negative regions or departments. For the purpose of this research, the method is limited to a discussion of a quantitative method to propose which steps to follow in order to derive a valid and reliable measuring instrument.

- *Time horizon*: Reactions to changes can be monitored over time by comparing data collected at different intervals [31]. A cross-sectional design (also called a survey design) entails the collection of data on more than one case, but at a single point in time across a number of variables [5]. This means that a cybersecurity culture can be assessed at a point in time, for example in year x and again in year y, but during a defined period (e.g. 2 weeks), using a questionnaire containing a number of variables (or dimensions). This will allow the researcher to detect patterns or associations and compare data between the survey of year x and year y to identify improvements and monitor change. Once a cybersecurity culture measuring instrument is validated, it can be reused to derive benchmark data and to perform cross-sectional and longitudinal studies.

- *Techniques and procedures:* Statistics refers to an approach in research whereby humans are studied and the information derived is analyzed using statistical or mathematical calculations [23]. Statistics are used in quantitative research methods to analyze survey data as well as in the questionnaire development to ensure its validity and reliability. Comparison is possible with the use of psychometric instruments (questionnaires) that have been normed and standardized, following rigorous validity and reliability testing [4]. Various comparisons can be made with regard to data on regions, departments, age, and other biographical traits. This allows the researcher to focus future interventions and even benchmark them against future survey data to analyze the impact of changes. It is therefore imperative that the questionnaire, which has been developed to measure cybersecurity culture, be validated and tested for its reliability.

V. The Proposed Cybersecurity Culture Research Methodology (CSecRM) and its Implementation

The proposed research methodology, cybersecurity culture research methodology (CSeCRM), to ensure a valid and reliable measuring instrument for conducting cybersecurity culture research, is portrayed in figure 4. The objective is to conduct cybersecurity culture research using a measuring instrument that is meaningful and powerful due to the statistical robustness that allows the researcher to draw conclusions and make predictions based on the data obtained [4].

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

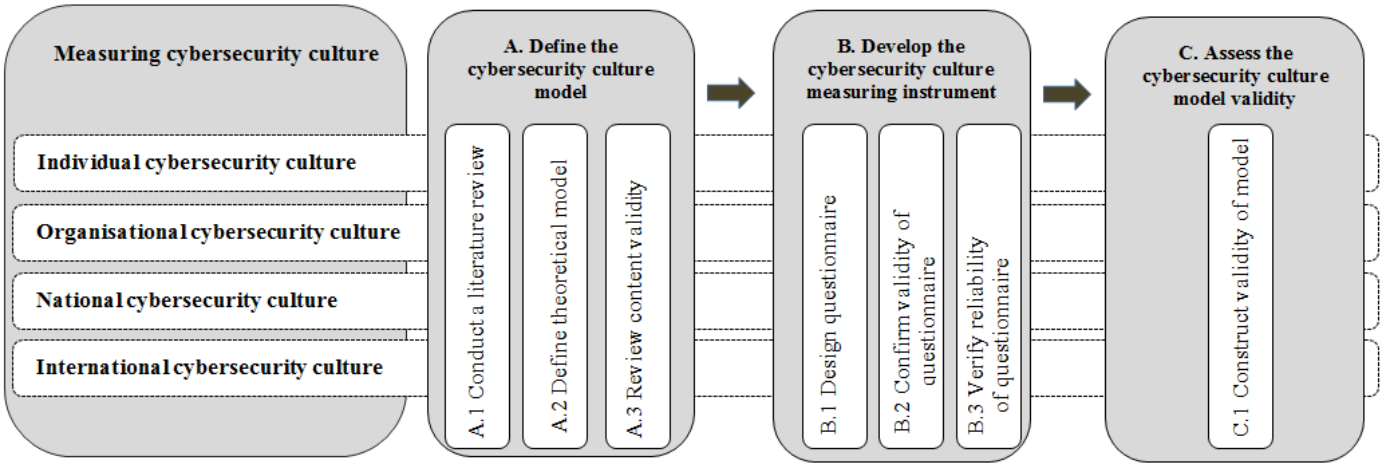

Fig. 4. Cybersecurity culture research methodology (CSeCRM)

The proposed methodology comprises three key phases (A, B and C) adapted from the structural equation model process of Hair, Black, Babin, and Anderson [18]. In phase A, a cybersecurity culture model is defined. However, in order to validate a model statistically, data are required that have been derived from a survey using a cybersecurity culture questionnaire developed in phase B. This is followed by phase C, where the validity of the cybersecurity culture model is determined. Figure 4 depicts the four levels of cybersecurity culture, indicating that phases A to C must be applied for each level of cybersecurity culture in order to measure each respective level to obtain a comprehensive view of cybersecurity culture.

Each of the phases will be discussed separately in the paragraphs below, including a discussion of the implementation thereof in a case study organization for illustration purposes. As such, the scope of the implementation is limited to an assessment of cybersecurity culture at organizational level, and not an individual, national or international level. The scope of the CSeCRM implementation is further limited to illustrate the application of the development of a reliable and valid measuring instrument (phases A and B) and hence, the results of the cybersecurity culture assessment are only discussed at a high level. Similarly, the statistical analysis of phase C is not discussed; however, the research work of Martins and Da Veiga [36] may be consulted for an illustration of structural equation modeling.

The cybersecurity culture assessment was conducted at two intervals in an international organization. This organization employed approximately 7,000 employees in 2010, which increased to just over 8,000 in 2013. At the time of the assessment, the organization had offices in twelve countries, namely Australia, Botswana, Guernsey, Hong Kong, Ireland, Jersey, Mauritius, Namibia, South Africa, Switzerland, the United Kingdom and the United States. In 2010 and in 2013, the questionnaire was sent out in electronic format to all employees, who had three weeks to complete the survey. Statistical analysis was conducted on the data to validate the questionnaire and to report back to the organization in terms of the proposed action plans.

The remainder of this section deals with the CSeCRM methodology and its implementation in the organization to illustrate how to derive a valid and reliable measuring instrument.

A. Define the cybersecurity culture model

1) Conduct a literature review

The purpose of the literature review is to gather preliminary information about important issues regarding the cybersecurity culture to be measured [6]. Interviews or group discussions can be used to identify key issues and give the researcher an idea of which questions to ask [53].

A literature review is critical to identify potential constructs that can be used to develop the cybersecurity culture questionnaire. It is important to remember that the same constructs cannot be used when measuring the cybersecurity culture of a financial organization, a university or a school, for instance. One would expect the concepts to be contextualized to the audience, where the cybersecurity culture is to be measured, as well as other aspects such as the regulatory environment and industry codes of conduct.

The research work pertaining to an information security culture model of Da Veiga and Eloff [9] was leveraged off and used as a reference for the focus group discussions to aid in identifying cybersecurity culture constructs. For the purpose of the case study organization, a focus group was formed with key employees, such as the information security officer. Important issues pertaining to cybersecurity culture in the context of the organization's business processes and policy requirements for end users when processing information were explored in the focus group.

2) Define the theoretical model

A theoretical model is defined to portray the important issues or topics (constructs) identified in the literature review and related activities [18]. The theoretical model typically incorporates key concepts, and identifies potential relationships and influences between the concepts. A cybersecurity culture model can thus be formulated depicting the key concepts to be measured. Such a model can be different for organizations in different jurisdictions or industries.

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

The information security culture model of Da Veiga and Eloff [9] was used as the baseline for identifying the cybersecurity culture constructs. Privacy of employee and customer data and the risks and use of social media in the context of cybersecurity were added. Mostly employee and customer data have been compromised in cyber attacks [43]. This introduces a risk to the protection of personal information and privacy of employee and customer data. The protection of personal information of customers is one of the biggest motivations for organizations to invest in information security [25]. As the case study organization was a financial institution serving customers, the information security officer specifically requested that these two constructs be added to the information security culture model in order to adapt it for cybersecurity culture.

3) Review the content validity of the model

Content validity evaluates the theoretical perspectives underlying the measuring instrument and the way in which the theory has been used to develop the items that are measured [4, 15]. In the case of the cybersecurity culture questionnaire, content validity can be confirmed by considering the definition of cybersecurity culture and components of the cybersecurity culture model.

If an existing questionnaire is used, content validity has to be established by validating the cybersecurity culture questionnaire against the cybersecurity culture definition, model, and related theory in order to determine the adequacy of coverage for each subject area. In other words, each construct in the cybersecurity culture model should be covered by a statement or question in the questionnaire to ensure that the results obtained from the assessment are valid and can be used to make decisions. This applies both to designing a completely new questionnaire and using an existing questionnaire. In addition, specialists in the field may be consulted during focus and discussion groups to further validate the constructs and content of the model [47].

The definition of cybersecurity culture incorporates the protection of the IT infrastructure and the individual in cyberspace. An organization should therefore have appropriate governance structures, policies, and processes in place to protect not only the IT infrastructure and information processed using it, but also their employees and customers. From a content validity perspective, the existing Information Security Culture Assessment (ISCA) model and questionnaire [9] incorporates aspects related to the protection of the IT infrastructure and information, but do not include specific constructs pertaining to the protection of the individual. By adding privacy and the use of cyberspace in an individual context, such as social media, the model was expanded to deal with content validity. Other concepts might be applicable when aiming to assess the cybersecurity culture at individual, national or international level, and hence the model should be re-examined in those scenarios.

B. Develop the cybersecurity culture measuring instrument

1) Design the questionnaire

The constructs identified in the theoretical model are used to design the cybersecurity culture questionnaire statements. The researcher may collect three types of data when doing a survey, namely opinion variables (i.e. how employees feel about cybersecurity and what they believe is true or false), behavior variables (i.e. what employees did in the past when using cyberspace, what they do now or what they will do in future), and attribute variables (i.e. characteristics of employees such as their age or grade) [13]. A distinction needs to be made between these concepts when formulating the questionnaire statements to ensure that the objectives are met. According to Hair, Black, Babin, and Anderson [18], a minimum of three, or at least four, items (statements or questions) should be developed per construct. Saunders, Lewis, and Thornhill [47] propose data requirement steps that can be used to compile questionnaire statements. These steps include defining investigative questions based on the research objectives, listing for each question the variables required to collect data to answer the question, and establishing the detail required for each variable after the measurement question has been developed. Numerous questionnaire principles must also be followed to ensure a reliable measuring instrument, such as asking only one question at a time, not using jargon, not using negative or double negative questions, not using questions that may imply a certain answer, etc. [6, 31].

To illustrate the implementation of CSeCRM, an existing information security culture measuring instrument was identified with the objective of adapting it for cybersecurity culture. The ISCA instrument [10] was therefore used, as it was designed to assess an information security culture from an organizational perspective, irrespective of the technology environment, and could therefore be extended to cyberspace. It is also based on the information security culture model developed by the researchers. The ISCA was adapted by adding privacy-related and social media questions, as identified in phase A.

The final questionnaire used to assess cybersecurity culture in the organization comprised eleven dimensions, namely information asset management, information security policies, change, user management, information security program, information security leadership, information security management, trust, training and awareness, privacy perception, and cybersecurity in practice.

Each of the dimensions comprised more than three statements per dimension, measured on a Likert scale (strongly agree, agree, unsure, disagree, and strongly disagree). The cybersecurity in a practice dimension consisted of “yes-no” (single-response) and multiple-response scales. The three types of data variables were considered in the design of the questionnaire and, as such, a separate knowledge section was added to the beginning of the questionnaire (section A). Section B dealt with the opinion variables and section C consisted of biographical questions.

Table 1 is an extract of some of the privacy and social media statements that were added.

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

TABLE I. EXTRACT OF QUESTIONNAIRE STATEMENTS

Statement
1. I understand what the Group's policy is on posting work-related information on social networking sites (Facebook, MySpace, Friendster, Twitter, LinkedIn, etc.).
2. I know what the risk is when opening e-mails from unknown senders, especially if there is an attachment.
3. I use my work e-mail address on social networking sites.
4. I have changed the default privacy settings of my account in social networking sites.
5. It is acceptable to me if employees were disciplined if they posted inappropriate comments about the Group on social networking sites.

a) Sample size

In order to generalize the findings of a cybersecurity culture survey across the population and to make recommendations, it is important to ensure that the sample is representative. The required sample must be calculated each time the cybersecurity culture survey is conducted. The sample size can be calculated using the overall population number (e.g. number of total employees across all twelve countries) and for groups (e.g. departments and regions) using the method of Krejcie and Morgan [33]. Following this approach, a sample is calculated on a marginal error of 5% and a confidence level of 95% to ascertain the findings across the population. It must be ensured that sufficient samples are obtained for the overall data and the various biographical groups.

The sample size for the organization was thus calculated using the overall staff numbers and for each department to ensure that representative responses were obtained. In 2010, 2,016 employees participated, while an overall sample of 364 was required. In 2013, a total of 2,159 employees participated, with a sample requirement of 367. Sufficient responses were therefore obtained, with a marginal error of 5% and a confidence level of 95% for both survey intervals.

2) Confirm validity of the questionnaire

Validity is a complicated statistical term, but necessary to consider in order to construct a powerful survey instrument 15]. The concept of validity implies that care must be taken to ensure that the questionnaire assesses what it claims to assess [3, 12, 15]. A valid questionnaire consistently yields reliable and stable results over time [12]. Reliability can be achieved without validity [24]. In other words, although results of a measurement can be reproduced and be consistent, the questions that are asked may be about irrelevant factors. The opposite is true for validity, where a measurement that is unreliable can never be valid. According to Brewerton and Millward [4], factor analysis can be employed to assess the robustness of the questionnaire's constructs (dimensions), thereby identifying clusters of questions and forming new constructs.

Factor analysis was conducted using the 2013 data for the dimensions where a Likert scale was used. Statements with a value greater than 0.3 were grouped into new factors (dimensions) [21]. Listed below are the new factors A to G, with the newly grouped statements based on the statement number as in the questionnaire:

- Factor A – 20 statements: 49, 55, 50, 54, 62, 35, 61, 58, 57, 28, 60, 22, 56, 24, 66, 64, 42, 21, 47, 32
- Factor B – 13 statements: 44, 43, 30, 36, 45, 29, 34, 38, 46, 53, 19, 27, 52
- Factor C – 5 statements: 26, 23, 39, 31, 33
- Factor D – 6 statements: 48, 63, 40, 20, 59, 41
- Factor E – 5 statements: 69, 65, 70, 67, 68
- Factor F – 2 statements: 71, 72
- Factor G – 3 statements: 25, 37, 51

A second-phase factor analysis was conducted to establish whether the statements in factor A could be further divided into sub-dimensions. As such, they were grouped into two new dimensions, namely A1 and A2.

- A1 – 12 statements: 54, 60, 64, 57, 49, 62, 61, 66, 50, 56, 42, 47
- A2 – 8 statements: 21, 28, 24, 22, 55, 35, 32, 58

3) Verify the reliability of the questionnaire

The purpose of examining Cronbach's alpha (item analysis) is to determine the reliability of a questionnaire and the degree to which the items selected "fit into" the intended area (cybersecurity culture) measured. The reliability figure obtained provides an indication of the level of consistency across the scale items [4] and varies between 0 and 1. Cronbach's alpha is used to examine the frequencies and descriptive statistics for each item on the survey across all responses obtained [6]. Items with a coefficient of between 0.6 and 0.7 can be accepted as an absolute minimum to be identified as a factor [4, 24]. This will help the researcher use statements that measure cybersecurity culture accurately.

TABLE II. CRONBACH'S ALPHA PER FACTOR

Factor	Cronbach's alpha
Factor A1	0,887
Factor A2	0,766
Factor B	0,878
Factor C	0,798
Factor D	0,803
Factor E	0,764

Cronbach's alpha was determined for the factors and it is depicted in table 2. Factors F and G were not included, as they only include two statements, and a minimum of three statements is required per construct [18].

C. Assess the cybersecurity culture model validity

1) Construct validity of model

The technique of structural equation modeling (SEM) can be used to determine the construct validity of the cybersecurity culture model. SEM involves the "amalgamation of multiple regression and confirmatory factor analytic techniques to assist in the assessment of developed models" [4]. It is suggested that a valid and reliable measuring instrument be used when assessing cybersecurity culture and that phase C be used to complement the validity of the cybersecurity culture model. As the focus of this paper is to illustrate how to implement

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

CSeCRM to derive a valid and reliable measuring instrument, the implementation of phase C is excluded.

D. Other statistical analyses

Further statistical analyses can be conducted to analyze the results of the cybersecurity culture survey with the objective of establishing the level of cybersecurity culture and determining whether it is acceptable. The most negative and positive constructs are identified to prioritize corrective actions and initiatives. Similarly, the most positive statements and most negative statements are identified to help design initiatives. Generally, the mean and standard deviation scores are used to identify these areas. The findings of the statistical analyses are typically incorporated in a report with key actions and a roadmap to enable, for example, an organization to implement suitable action plans.

The statistical results indicated on the overall mean score that the cybersecurity culture level was 4.10 in 2013, being an improvement from 3.76 in 2010. The average of the additional privacy statements improved from 3.46 in 2010 to 3.56 in 2013. It is interesting to note that 27% of employees felt that access to social networking sites would enhance their working activities, while only 8.1% of employees used their work e-mail address on social media (21.5% in 2010). However, only 52.1% indicated that they would feel comfortable if the group monitored what they posted on social media networking sites. The most negative dimensions were identified as trust, management, and leadership. The most positive dimensions were identified as asset management, policies, and change. In conclusion, it was found that the mean scores for the dimensions and individual statements improved from one assessment to the next, indicating that a more positive cybersecurity culture was being fostered. The CSeCRM can be used as a research methodology to develop the cybersecurity culture questionnaire. It can also be applied when conducting a cybersecurity culture survey after the questionnaire has been validated to monitor and improve the culture continuously through metrics that can be benchmarked to the previous survey(s). It is often necessary to repeat the statistical analysis, as researchers might find that the validated questionnaire might have to be customized for the audience each time a survey is conducted in a different environment, which then necessitates a repeat of the validity and reliability tests.

VI. CONCLUSION

This research paper set out to define cybersecurity culture and to propose a research approach and methodology to develop a valid and reliable cybersecurity culture measuring instrument. The application of the proposed cybersecurity culture research methodology (CSeCRM) was illustrated in the context of a case study in an international financial organization.

In answering the first research question, a cybersecurity culture was defined as the intentional and unintentional manner in which cyberspace is utilized at four levels, namely at international, national, organizational or individual level, which either promotes or inhibits the safety, security, privacy, and civil liberties of individuals, organizations or governments. The second research question focused on proposing a research philosophy and approach that can be followed to measure a cybersecurity culture. As such, a positivist philosophy, employing a quantitative method, was proposed, consisting of a survey strategy whereby statistical analysis can be conducted to analyze the data and determine the cybersecurity culture level

The main contribution of this research is the CSeCRM that can be applied to develop a valid and reliable cybersecurity culture measuring instrument for each of the four levels of cybersecurity culture. The assessment of the cybersecurity culture level can be incorporated in existing information security risk management and incident management frameworks to understand the risk from a human perspective in, for example, an organization. This can complement motivations for reduced cyber risk insurance if the culture is at an acceptable level; it can also be used by governments as input to define a cyber strategy to mitigate risks from a user perspective. Furthermore, it can enhance incident response decision frameworks to predict incidents from a user perspective. Organizations can use the assessment data to target cybersecurity awareness and training for employees in specific departments or regions where the culture is not acceptable. It can aid in directing budgets and can also serve as motivation to management for resources to address developmental dimensions identified in the assessment. Furthermore, the cybersecurity culture assessment data can be benchmarked year on year to track changes in the culture and to determine if action plans were successful to change the cybersecurity culture and thereby aid to minimize the risk of the human component in cyberspace.

Further research work will be conducted to develop a cybersecurity culture model comprising the four levels that can aid in informing a comprehensive measuring instrument for each level. Structural equation modeling will also be applied to further enhance the validity of the proposed model. This will aid in having a standardized measuring instrument that can be utilized from an international, national, organizational, and individual perspective to measure the cybersecurity culture, in an attempt to minimize the risk that human behavior poses to ensuring a safe cyberspace.

REFERENCES

[1] P. Baltzan, Business Driven Technology, 5th ed., New York: McGraw-Hill Irwin, 2006.

[2] N. Ben-Asher and C. Gonzalez, “Effects of cyber security knowledge on attack detection,” Comput. Hum. Behav., vol. 48, pp. 51–61, 2015.

[3] M. L. Berry and J. P. Houston, Psychology at Work, Wisconsin: Brown and Benchmark, 1993.

[4] P. Brewerton and L. Millward, Organizational Research Methods, London: Sage, 2002.

[5] A. Bryman, Social Research Methods, 4th ed., New York: Oxford University Press, 2008.

[6] A. H. Church and J. Waclawski, Organizational Surveys – A Seven Step Approach, San Francisco: Jossey-Bass, 1998.

[7] Cybercrimes and Cybersecurity Bill, Draft for public comments. B2-2015. [Online]. Available: http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf. [Accessed: 13 October 2015].

[8] A. Da Veiga, Cultivating and assessing an information security culture. PhD dissertation, University of Pretoria, 2009.

[9] A. Da Veiga and J. H. P. Eloff, “A framework and assessment instrument for Information Security Culture,” Comput. Secur., vol. 2010, no. 29, pp. 196-207, 2010.

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

[10] A. Da Veiga and N. Martins, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," Comput. Secur., vol. 2015, no. 9, pp. 162–176, 2015.

[11] M. R. De Villiers, "Models for interpretive information systems research, part 1: IS research, action research, grounded theory – a meta – study and examples," in Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems, M. Mora, O. Gelman, A. Steenkamp, and M. S. Raisinghani, Eds. Hershey: IGI Global, 2012, pp. 222-237.

[12] W. R. Dillon, J. T. Madden, and N. H. Firtle, Essentials of Marketing Research, Boston: Irwin, 1993.

[13] D. A. Dilman, Mail and Internet Surveys: The Tailored Design Methods, 2nd ed., New Jersey: Wiley, 2007.

[14] Electronic Communications Act (ECTA), 2005, [Online]. Available from: http://www.acts.co.za/electronic-communications-act-2005/index.html [Accessed: 05 May 2015].

[15] A. Furnham and B. Gunter, Corporate Assessment: Auditing a Company's Personality, London: Routledge, 1993.

[16] L. A. Gordon, M. P. Loeb, and T. Sohail, "A framework for using insurance for cyber-risk management," Commun. ACM., vol. 46, no. 3, pp. 81-85, 2003.

[17] S. Haag and M. Cummings, Management of Information Systems for the Information Age, 9th ed., New York: McGraw-Hill Irwin, 2013.

[18] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, Multivariate Data Analysis, A Global Perspective, 7th ed., Upper Saddle River: Pearson, 2010.

[19] Y. He, L. A. Maglaras, H. Janicke, and K. Jones, "An industrial control systems incident response decision framework," IEEE Conference on Communications and Network Security (CNS 2015), Florence, Italy, 2015.

[20] D. Hellriegel, Jr, J. W. Slocum, and R. W. Woodman, Organizational Behaviour, 8th ed., Cincinnati, OH: South-Western College, 1998.

[21] J. L. Hintze, Number Cruncher Statistical Systems (Version 5.03 5/90), Kaysville, UT: NCSS, 1995.

[22] Homeland Security, A roadmap for cyber security research. 2009. [Online]. Available: http://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf. [Accessed: 23 September 2015].

[23] D. C. Howell, Fundamental Statistics for the Behavioral Sciences, 8th ed., Belmont CA: Wadsworth Cengage Learning, 2014.

[24] G. K. Huysamen, Sielkundige Meting – 'n Inleiding, Pretoria: Van Schaik, 1988.

[25] Information Security Breaches Survey – Technical Report, 2015. Conducted by PwC in association with Infosecurity Europe. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf. [Accessed: 23 September 2015].

[26] ISACA and RSA, An ISACA and RSA Conference. State of Cyber Security: Implications for 2015. [Online]. Available: http://www.isaca.org/cyber/Pages/state-of-cybersecurity-implications-for-2015.aspx [Accessed: 22 September 2015].

[27] ISO/IEC 27002:2013, Information Technology E Security Techniques E Code of Practice for Information Security Management, Kay Westlake: BSI, 2013.

[28] Joint Staff US Army, Cyberspace Operations. The Defense Technical Information Center, 2013. [Online]. Available: www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf [Accessed: 23 September 2015].

[29] F. Karlsson, J. Aström, and M. Karlsson, "Information security culture – state-of-the art review between 2000 and 2013," Infor. & Comput. Secur., vol. 23, no. 3, pp. 246-285, 2015.

[30] P. Kornelisse, K. Wolters, D. Van Ham, R. Heil, H. Oymans, S. Hegt, and T. Kipp, The five most common cyber security mistakes, 2013. [Online]. Available: http://www.kpmg.com/NL/en/Issues-And-Insights/ArticlesPublications/Pages/The-five-most-common-cyber-security-mistakes.aspx [Accessed: 29 July 2015].

[31] A. I. Kraut, Organizational Surveys, San Francisco: Jossey-Bass, 1996.

[32] R. Kreitner and A. Kinicki, Organizational Behaviour, Chicago: Irwin, 1995.

[33] R. V. Krejcie and D. W. Morgan, "Determining sample size for research activities," Educ Psychol Meas., vol. 30, pp. 607-610, 1970.

[34] E. Luiijf and K. Besseling, "Nineteen national cyber security strategies," Int. J. Crit. Infrastruct., vol. 9, no. 1.2, pp. 3-31, 2013.

[35] O. Lundy and A. Cowling, Strategic Human Resource Management, London: Routledge, 1996.

[36] N. Martins and A. Da Veiga, "An information security culture model validated with structural equation modelling". Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), 2015, pp. 11-22.

[37] McAfee and SAIC, Underground economies. Intellectual capital and sensitive corporate data now the latest cybercrime currency, 2011. [Online]. Available: http://freepdfs.net/rp-underground-economies-national-defense-industrial-association/dd8111e5875c655df5def936e6110948/ [Accessed: 22 September 2015].

[38] National Institute of Standards and Technology (NIST), Framework for improving Critical Infrastructure Cybersecurity, Version 1.0, 2014.

[39] Organisation for Economic Co-operation and Development (OECD), Guidelines for the security of information systems and networks – towards a culture of security. [Online]. Available: www.oecd.org/internet/ieconomy/15582260.pdf [Accessed: 22 September 2015].

[40] Organisation for Economic Co-operation and Development (OECD), Working Party on Information Security and Privacy, The promotion of a culture of security for information systems and networks in OECD countries, 2000. DSTI/ICCP/REG(2005)1/FINAL. 2005. [Online]. Available: www.oecd.org/internet/ieconomy/35884541.pdf [Accessed: 22 September 2015].

[41] C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, Security in Computing, 5th ed., Massachusetts: Pearson Education, 2015.

[42] Ponemone Institute. Global Cyber Impact Report, 2015. [Online]. Available: http://www.aon.com/risk-services/thought-leadership/2015-global-cyber-impact-report.jsp [Accessed: 22 September 2015]. PricewaterhouseCoopers (PwC), The global state of information security survey, 2014. [Online]. Available: http://www.pwc.com/gx/en/consulting-services/information-security-survey/ download.jhtml [Accessed: 20 September 2015].

[43] K. Rainer and H. Watson, Management Information Systems, Moving Business Forward, New Jersey: John Wiley & Sons, 2012.

[44] K. F. Rauscher and V. Yashenko (Eds.), Critical Technology Foundations, EastWest Institute: London, 2011. [Online]. Available: http://www.eastwest.ngo/idea/russia-us-bilateral-cybersecurity-critical-terminology-foundations [Accessed: 22 September 2015].

[45] S. Robbins, Organizational Behaviour, 9th ed., New Jersey: Prentice Hall, 2001.

[46] M. Saunders, P. Lewis, and A. Thornhill, Research Methods for Business Students, 5th ed., Essex: Pearson Education, 2009.

[47] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," Comput. Secur., vol. 2016, no. 57, pp. 14-30, 2016.

[48] E. H. Schein, Organizational Culture and Leadership, San Francisco: Jossey-Bass, 1985.

[49] T. Schlienger and S. Teufel, "Tool supported management of information security culture: An application to a private bank," in The 20th IFIP International Information Security Conference (SEC 2005) - Security and Privacy in the Age of Ubiquitous Computing, R. Sasaki, E, Okamoto, and H. Yoshiura, Eds. New York: Springer, pp. 65-75.

[50] G. B. Shelly, T. J. Cashman, and H. J. Rosenblatt, Systems Analysis and Design, 6th ed., Boston: Thomson Course Technologies, 2006.

[51] R. Von Solms and J. Van Niekerk, "From information security to cyber security," Comput. Secur., vol. 2013, no. 38, pp. 97-102, 2013.

[52] M. Walters, Employee Attitude and Opinion Surveys, London: Institute of Personnel and Development, 1996.

978-1-4673-8460-5/16/$31.00 ©2016 IEEE