Information Security Culture: A General Living Systems Theory Perspective

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

Karen Renaud
Computing Science
University of Glasgow
Glasgow, Scotland
Karen.Renaud@glasgow.ac.uk

***Abstract*—Information security culture (ISC) is often acknowledged as being a vital subculture within an organizational culture. As a subculture, its purpose is to fulfil its security purpose, while integrating into, and supporting, the broader organizational culture. However, in contrast, few discussions of ISCs acknowledge that the ISC itself is comprised of subcultures. The research literature's lack of exploration of this nested nature of ISC may be hindering in-depth understanding of the ISC as a system within itself, as well as within the broader organizational culture. This paper will therefore address this by straying from traditional views of ISCs. We will examine an ISC as a self-managing, self-repairing collective of multiple ISCs which meet the organizational culture's security needs. The paper's objective is to show that an ISC can be viewed and understood as a living system.**

Keywords-information security culture; general living systems theory, conceptual

I. INTRODUCTION

Many organisations acknowledge that the creation of an acceptably effective information security solution is of vital importance [1]. Information security aims at securing the processes, technology and people involved with the information used in the activities that fulfil the business's corporate objectives. These processes, technology and people form the components of such an information security solution and accordingly have to be managed [2].

Employee actions and behavior are particularly important in an information security solution, as almost all information security solutions rely, to a certain extent, on the humans involved in the security process making the right decisions and acting securely [3]. While technology and processes can be formulated so as to be theoretically secure, the true level of security of such technology and processes relies on the people involved in their use and implementation [4]. The extent to which people use technology securely and comply with the mandated secure processes can drastically affect how truly secure these components are.

People can both consciously and unconsciously become a threat to any information security solution [5]. When they become a conscious threat it may be with a specific intent or because of negligence. Alternatively, when they become an unconscious threat it may be for a range of reasons, including a lack of knowledge of security practices, an inability to properly apply their knowledge to their own work role or environmental context, because they have been conned or due to common negligence. Regrettably, as a result of this it is more likely that a breach that occurs in an information security solution is the fault of humans, and not technology [3]. This threat has become known as the "human factor" in information security.

The establishment of an organizational information security culture (ISC) has been widely accepted as the appropriate counter to this "human factor" threat [4]. The theory supporting this solution being that the creation of a security-conscious corporate culture could potentially lead to employees adopting secure, work-related behavior as a behavioral default [1], [5].

An ISC is often acknowledged as being a subculture of the larger organizational culture [1]. However, it is rarely acknowledge that it can have subcultures of its own. ISCs are, typically, presented in literature as single-level conceptual constructs which are uniformly applicable to all aspects of an organization. However, this representation may be too simplistic to explain the interactions between the interconnected secure business activities and the components of a comprehensive organizational ISC. Therefore it may be advantageous to examine an alternative view if ISC.

An ISC *could* be viewed as a collection of nested systems that display emergent properties and are also self-maintaining and self-repairing. These properties match the primary characteristics of general living systems. This paper will thus examine an ISC to determine whether it may be viewed as a living system.

Living systems are open, complex, adaptive, self-organizing living entities that interact with their environment or other systems [6]. A living systems perspective will not simplify how we view ISCs. In fact, it will likely complicate it. However, it is our belief that this alternative view of an ISC will reveal considerations of the culture that previous models have failed to identify. This new perspective may therefore assist in developing a further understanding of the underlying components, operations and impact of an ISC. It may enable us to better understand and predict the overall culture and how the organizational and security cultures interact. This, in turn, may affect our understanding of how good ISCs ought to be nurtured and encouraged.

The paper will begin by briefly discussing the concept of ISC; then it will provide a brief overview of general living systems theory and, finally, it will present the way in which an

The financial assistance of the Vodacom/NMMU and National Research Foundation (NRF) scholarships in this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the authors and are not necessarily to be attributed to the sponsors.

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

ISC could be viewed as a general living system by mapping culture to the system characteristics.

II. INFORMATION SECURITY CULTURE (ISC)

Culture is broadly considered to be the overall, taken-for-granted assumptions that a group has learnt throughout history [7]. ISCs build on this premise.

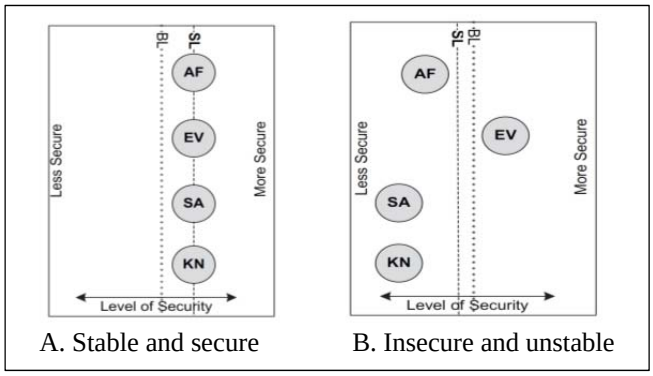
Many current authors deal with the topic of an information security culture ([8][9][10],[11], [12],[13], [14]). Most of these authors focus on cultivating, assessing or auditing a culture. To achieve this the authors commonly base their views' understanding and representation of an ISC on adaptions of Schein's three-tier organizational culture model [1]. The tiers in Schein's model consist of underlying assumptions, espoused values and artifacts [7]. However, the model deals with organizational culture in general, not ISC specifically, and the authors cited here seldom provide in-depth explanations about how their interpretation of the adapted model translate to the context of information security. This has left much about the practice to be subjectively interpreted. Van Niekerk and Von Solms have bridged this gap in knowledge by presenting a conceptual model of an ISC and have focused on explaining how its underlying components and processes could influence one another [4]. As a result of the comprehensiveness of the definition, the focus on the conceptualization of an ISC, and the degree of relativity of the explanation of the interactions to the purpose of the research, this paper will adopt their definition of an ISC.

Van Niekerk and Von Solms's definition of an ISC derives from, and expands on, Schein's organizational culture model. Schein lists artefacts, espoused values and knowledge as dimensions of his culture model [7]. 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 [7]. This knowledge dimension was included as the authors theorized that in order to successfully foster an ISC (as a sub-culture within an organizational culture), all business activities would need to be performed in a secure way [12]. Adequate information security knowledge and skills were therefore deemed essential to enable an employee to be able to perform any business activity in a secure manner [4]. According to their conceptualization, an ISC thus consists of four information security related components, namely, artefacts, espoused values, shared tacit assumptions and knowledge [4].

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 refers 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 are deemed to be "measurable but hard to decipher" [4].
2. Espoused Values (EV) – The guidelines for what to include in a policy, and the subsequent ISC, in order 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 [4].
3. Shared Tacit Assumptions (SA) – The beliefs and values of the individual and collective employees. These include 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 [4].
4. Knowledge (KN) – The necessary and required levels of information security specific knowledge needed to perform the daily business tasks in a secure manner [4].

Within this framework, Van Niekerk and Von Solms explain how these components of an ISC can affect one another [4]. It is necessary to understand these interactions in order to be able to be able to predict the strength, stability and predictability of an ISC. Figure 1 illustrates an example.



A. Stable and secure B. Insecure and unstable

Figure 1: Comparison of a stable, secure culture and an unstable, unsecured culture

Figure 1 shows the interactions of an organization's ISC components and their effect on the strength of that particular ISC. The line labelled BL represents this case's minimum acceptable security baseline (BL). The side on the left of BL indicates a culture and a set of artefacts that are less secure than the desired minimum BL. The opposite is applicable to the right side of the BL. The EV, SA and KN culture components can fall on either side of the baseline. The closer the components are aligned, the more stable the culture is. The consistency of the component strengths determines the strength of the culture. Figure 1 part A shows a culture with well-aligned, strong components. Consequently, the net security level line (SL) of the culture indicates that the combined net effect of all four culture levels is stable and secure. In comparison Figure 1 part B shows a culture with strong EV, a lack of suitable KN, and a lack of the preferred SA. This results in the AF being measured as unsecured. The resultant internal opposition of the culture components results in the culture's net effect being unsecured and unstable.

This basic explanation of an ISC framework and its components enables us to comprehend the overall conceptual construct of the high-level ISC within the organizational culture. However, this view may be overly simplistic.

We argue that an ISC exists at many levels and in many forms within an organization. It is the detailed ISC components, context and data within each of these individual

and collective subcultures that actually reflect the organization's true ISC strength and effectiveness. Consequently, the sole use of an aggregated view of an ISC cannot reveal the true, subtle levels of innateness, integration and strength in an organization's ISC.

An ISC is only as strong as its weakest link. For example, having an aggregated strong password security culture is meaningless if the password security culture in a high-risk department is weak. In such a context it is possible that, as a subculture, the department's weak password culture could influence the culture of the entire organization. This example demonstrates how different contexts and levels of security can affect the overall ISC. Schein acknowledged the importance of context for an organizational culture. This acknowledgement is also valid for an ISC (as a subcomponent of an organizational culture) and its subcultures.

Schein noted that organizational culture is typically stable and resistant to change [7]. This is partly because culture is the net result of many underlying factors. These same factors will also influence the way culture propagates. Therefore, in order to understand how culture propagates through an organization, one has to understand its context and relationships. This is also true for subcultures such as an ISC. Therefore, there is a need for a view or perspective that acknowledges this interconnection and interdependent nature of an organization's culture and ISC and the components of the ISC. This is particularly important in order for us to understand how the interconnected nature of the organization's culture and the SC component, and their various contexts, allow for and affect the development, propagation, maintenance, condition and emergent properties of all the cultures. Essentially, these cultures need to be viewed as self-maintaining and self-propagating systems. A theory which may be appropriate for modelling such a view is general living systems (GLS) theory.

To determine whether this view is possible, this paper will briefly examine a GLS and its characteristics. It will then determine whether the main characteristics of the GLS align with that of an ISC.

III. General Living Systems Theory

GLS is a systems theory presented by James Grier Miller in his 1978 book *Living Systems*. The theory addresses a specific subset of systems, namely, *living* systems. Miller explores how phenomena occur by examining the relationships a system (organism) has with its environment (possibly a larger organism or system.)

A GLS is defined as being an open, complex, adaptive, self-organizing living system consisting of subsystems that interact with their environment or other systems by processing specific inputs, throughputs and outputs of various forms of matter energy and information [6], [15]. Each of these systems and subsystems can therefore be characterized as *purposeful* [6].

All living systems comply with the propositions of this definition, whether composite living systems (system of systems) or living subsystems.

A living system consists of many similar components (molecules or subsystems) which evolve and combine to make a larger, increasingly complex, suprasystem. Miller proposed that living systems could be divided into eight hierarchical levels, namely, cells, organisms, groups, organizations, communities, societies and supranational systems [15]. Each level increases in complexity and is considered higher than its predecessors as it is a compilation of its lower systems. Each composite system is therefore a suprasystem. Each level and system has its own typical structure and processes which serve the purposes of its own and its hosting environment (or system).

A GLS is therefore typically considered to be a complex entity. It is a system of systems. Each of these systems has a purpose, a process for fulfilling this purpose and a relationship with its environment which helps it fulfil its purpose while receiving from it what is needed by another system to fulfil its purpose.

The detailed explanation of exactly how all of this happens and how a GLS exists and lives is beyond the scope of this paper. Instead, this paper will examine whether ISC can be represented as a GLS when comparing it to some of the primary characteristics of a living system (as described by Miller). These characteristics will therefore be briefly explained and then mapped to an ISC in the next subsection.

IV. Mapping Information Security Culture to the Main Characteristics of a General Living System

Miller identified a number of key characteristics for a living system. This section will briefly outline five of these primary characteristics.

A. General living sytems follow a charter

Miller states that GLSs either contain genetic material composed of deoxyribonucleic acid (DNA), presumably descended from some primordial DNA common to all life, or have a charter [15]. In the case of an information security the latter would be the case.

A charter is the equivalent of a template, original "blueprint" or "program", which guides the creation of the living system's structure and process from the moment of its origin. Essentially, it is the general plan for the system's development and operation.

The charter describes the overall system's purpose and how the system will fulfil this purpose. In terms of an ISC, the authors would like to propose that the primary components of an ISC, namely, the espoused values (EV), artefacts (AF), shared tacit assumptions (SA) and knowledge (KN), map directly to this GLS characteristic.

The ISC components act as a guideline for the structuring of any ISC to fulfil a particular purpose. This is true for high/abstracted levels within an ISC as well as more detail-intensive levels. Basically, they provide the system boundaries and structure. The overall ISC culture has a specific purpose and plan of function and these are the original abstracted ISC components. Derived from this plan, any ISC and its subcultures follow the abstracted charter's (components) directives while implementing its solution/ contribution to the

charter's fulfilment in a manner which is context-specific to the implementation requirements of its environment.

The plan within the charter (the ISC components) includes guidelines for the creation, implementation, maintenance and possibly governance of the system. Essentially, it guides the system's development and growth and acts as a baseline according to which these design and implementation decisions may be measured. As a result of this role, the ISC charter and the abstracted ISC components may be considered to be both the system's charter and the "decider" subsystem in a living ISC.

B. General living systems have a decider subsystem

Within a living system there are a number of critical subsystems which were identified by Miller. Twenty of these essential systems were identified. Owing to limited space, this paper will only focus on the decider subsystem, which in the authors' opinion is the most relevant. The remaining subsystems, and how they map to the ISC, will be addressed by future work.

In a GLS there exists a "decider" subsystem. This is an essential, critical subsystem that controls the entire system, causing its subsystems and components to interact. It is necessary because without it there would be no interaction and with no interaction under decider control there is no system.

In the context of an ISC, the decider is the decision-making ability needed to initiate and manage the creation, maintenance or change of an ISC. This decision-making ability is representative of the underlying culture change processes which provide the decider with the facts (knowledge) needed to make effective and efficient decisions. This is therefore the representative of the decider subsystem. For an ISC, the culture change process involved in providing the decider with knowledge and decision-making capabilities comprises the various activities involved in fostering a culture, that is, the ISC fostering process. The ISC fostering process is therefore a very necessary part of the forming view of ISC from a GLS perspective.

The fostering process is designed to align the actual ISC with the desired ISC. This means that it is a process which makes decisions to trigger processes and activities which will result in the plan/charter for the system being fulfilled. How this is done will now be briefly discussed.

Fostering a strong ISC involves aligning the ISC dimensions (as previously explained in section II). In order to foster a culture and align the components of an ISC, change is required. Change is not uncommon within an organization, as it is necessary to ensure its continuity. Schein recognized the necessity of the change process at a cultural level [7]. He therefore proposed a structured change management process which aimed to facilitate an organizational culture change. Many authors have adapted this culture change; this paper will use an adaption discussed by Okere, Van Niekerk and Carroll [16].

This structured change management process consists of eight steps (shown in figure 2). These steps are as follows:

1. *Obtain top management support and commitment*. This is the stage in which (as a response to a specific business problem and context) the top management levels are decided to gain an understanding of the existing cultures, and acknowledge and commit to any existing necessary changes [16]. In order to accomplish this, management's understanding of the culture would require knowledge of the existing culture's existing AFs, EVs, SAs and KN. Only then could management declare new espoused values.
2. *Define the specific business problem*. This is the stage in which the current culture is analyzed and the preferred *new* culture is defined. The gap between the two culture states is also analyzed and the required steps to start the needed transformative process (unfreezing, learning and refreezing of concepts) are defined [16]. This is the stage in which the current and desired ISC dimensions would be compared.
3. *Develop strategic action plan*. This is a self-explanatory stage in which plans for the many steps within the transformative process are planned, for example the identification of required action and behavior changes, education plans, awareness and support encouragement [16].
4. *Create a cultural fit*. This is where a cultural fit is facilitated using mechanisms such as education, training and reward systems [16]. This stage would be where the actual execution of the plans and decisions would begin. Further, more detailed, implementation would then be executed via the next four stages of the process.
5. *Develop and choose a change leader team*. This is the stage which ensures that the individuals involved have a common purpose [16]. This could happen at a single or multiple levels of the culture.
6. *Create small wins*. The stage where important actions and steps within the process are identified as markers that will indicate the desired culture change [16]. These markers are used to motivate employees [16]. One of the aims of this stage would be to try involving everyone in the fostering process.
7. *Identify metrics, measures and milestones*. This involves the identifying of metrics to measure success and track change [16]. This stage logically follows its predecessor and aids in determining whether the decisions being made and implemented are having the desired result.

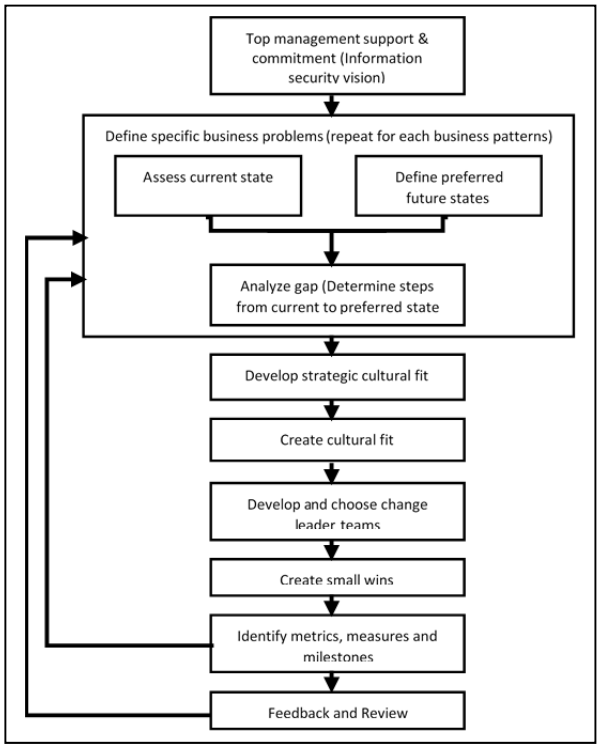


Figure 2: Adapted framework for culture change[16]

8. *Feedback and review*. The receiving of indicators from internal and external factors that may indicate the state of the culture and whether further change is required [16]. Indicators should include new measurements and estimation of SA, KN and AFs which have resulted or changed because of the changes made to comply with the EVs.

This change management process is the desired decision activity that aids the alignment of an ISC's dimensions. The entire change or culture fostering process is a continuously iterative, scalable model which may be applied within many a context. This process is an essential component of a living ISC system, as it enables all ISC living system activities and communications. Without this process the ISC would not be a living system as no communication would occur between ISC dimensions.

Besides being the charter and decider subsystem, this aspect of an ISC fostering process is also what enables another of a living system's characteristics, namely, its ability to self-repair and self-maintain. This characteristic will be briefly explained by the next section.

C. General living system can self-repair and self-maintain

One characteristic of living systems that is particularly important is its ability to self-repair and self-maintain provided the necessary components are in place. This is an important and necessary characteristic in order for a system to maintain a level of constancy over time [6], [15].

Within a living biological system self-repair and maintenance take place according to the following points: information processing, energy processing, material processing, synthesis of parts by combining materials, rearrangement and connection of disarranged parts, energy storing for fuel reserves and necessary structure, and removal of worn parts [6]. In a non-biological living system this can be similarly identified in the fostering process of an ISC (discussed in previous section). To ensure that an ISC corresponds with the organization's overall target and the targets of the various other subcultures, an ISC must be created, maintained and changed continuously [1]. How these map to one another will now be briefly explained.

Firstly, the synthesis, rearrangement, removal and replacement of parts indicates that, at this point, aspects of what works in a system are combined with other aspects that work from the same or another system, thereby replacing components that do not work and are no longer required. In the ISC fostering process this would occur throughout the entire process, while the process attempts to change/evolve the existing ISC and its components into the desired ISC and its desired components. For example, in order to meet the desired EV, the desired SA, KN and AFs would have to be created. This would not necessarily be a process which begins without an existing basis. For example, in an ISC fostering process, as previously discussed, the existing SAs, KN and AFs may start to be examined for compliance with the EVs of the desired ISC. The components of the existing dimensions that complied would then be then reused and possibly modified and/or expanded upon. This process could potentially mesh components from multiple implementations of the ISC (to be explained in section E) so as to obtain the best result.

Within the detailed implementation of this process it could be argued that the artefacts and resources allocated to the culture-fostering process would be equivalent to the energy, information and material needed for the system's processing activities. This would include all the activities and resources allocated, expended and created within the processes to alter the AFs, SAs and KN to match the ISC's desired EVs and other components. The resultant ISCs at the various levels of the living ISC system would be considered the energy stored for fuel reserves and the necessary structure, as this is what will facilitate future changes while itself being the existing cultural structure/product. A further in-depth examination of how exactly the resource allocation, use and processing activities map to the GLS processing activities will form part of future work.

The EVs, SAs, AFs and required KN change as the people, processes, technologies and suchlike governed by them or generating them change. This is taken into consideration within the fostering process by means of the feedback process. Therefore, they are considered part of the ISC – not external to it. Taking this into consideration, as well as the self-repair and self-maintenance points discussed, it is clear that an ISC is capable of, and is already, self-repairing and self-maintaining. The fostering of a culture entails the repairing and maintenance of that culture. However, whether the fostered ISC stabilizes and is adopted in a manner which ensures that the culture remains in a state that aligns with the desired EVs and so on is debatable. This debate will be addressed in future work.

Having now discussed the abstract charter (planned), and the decisive and self-maintenance characteristics of a culture, it is now necessary to understand the characteristics of a living system that actually implement/execute what is facilitated by those that have been previously discussed. The first of these characteristics to be discussed details the way a culture, as a system, works.

D. General living systems are open systems with significant inputs, throughputs and outputs of various sorts of matter – energy and information.

This section will provide the simplest explanation possible for how an ISC, on a functional level, exhibits the classic behavior of a living system. Firstly, an understanding is required of how a GLS functions.

Any GLS system is defined by its boundary. All system activities occur within the system boundary; anything outside it is considered the system's environment. Within the system boundary a constant flow of information, energy and matter into, through and out of the system is maintained [6]. This flow enables the system to fulfil its purpose. Living systems import matter/energy, as well as information, as input from its environment [6]. What is included in the types of received input is generally selective (relevant to systems purpose). These inputs are then used in the system's throughput ("metabolism") process.

In biological living systems this metabolism consists of thermodynamic energy processing and information processing [6]. The thermodynamic energy processing component of the metabolism format provides the "energy required for important activities such as reproduction, production and repair" [6]. The information processing aspect of the metabolism enables continuous information exchange over the system boundary (information processing). It is the information processing and each system's focused programmed decisions which help to regulate, adjust and control the way the thermodynamic processing occurs [6]. As a result of this, information processing therefore regulates the system's internal stresses and external strains, while allowing the system's purpose to be fulfilled [6].

During the metabolism/throughput process the system obtains/creates what it needs as well as some products or by-products. The system's purpose is fulfilled when the processing (throughput and transformation) creates a product which is specific to the system. Thus, once the internal processing procedures are complete, the system exports its specific product output into the system's environment where it is absorbed or collected by another system [6].

The GLS system will maintain a steady state of negentropy even though entropic changes occur in them. This happens because they take in inputs of higher complexity or organization or negentropy than their outputs. This difference permits them to restore their own energy and repair breakdowns in their own organized structure. This is a continuous process because, while the system releases its output, it simultaneously absorbs new input (matter/energy /information) from the resources in the environment [6]. This reabsorption of energy allows the system to continue its metabolism, self-maintenance, and self-repair processes.

In summary, a GLS functions by absorbing inputs from its environment, processing these inputs within the system boundary to obtain/create what the system requires, and then re-feeds any products or by-products of the processing back out into the systems environment [6]. This functional process can be found in the operation of an ISC.

In an ISC, the culture has expected inputs, namely, the EV and the SA and the existing culture's AFs (mostly the daily work process). These inputs are absorbed into and processed in the ISC fostering system. The EVs come from top management and the SAs come from the employees or users. Both the EVs and the SAs may be considered the information inputs absorbed by the system. They are processes and they regulate the ISC's process, which is equivalent of a GLS's thermodynamic processing. The existing culture's AFs, such as the daily work processes and procedures, are the equivalent of a GLS's matter/energy input imports. The processing of them to create a more secure culture for this system's particular context that meets the requirements within the EVs, which were its input, is the ISC's equivalent thermodynamic processing. The products which are created within the ISC system are role-based business behavior processes, and procedures which are not secure according to the current cultures EVs, SAs and KN. The conceptual map of how this processing occurs is shown in Fig. 3.

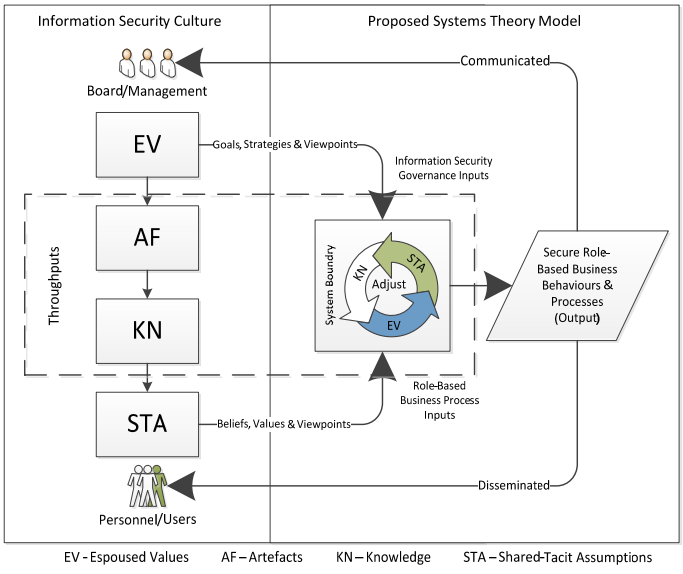


Figure 3: The input, throughput, output process of a living information security culture system

The negentropy within this system is displayed where the ISC system takes in the abstract EV and AF, uses the SA and KN of its context's SA and KN, creates a culture that is relevant to its own system, and then outputs the ISC AFs that are needed in its environment or other ISC systems.

This explanation abstractly describes how the functions of a GLS can be seen in a single instance of an ISC. However, it is important to note that the exact, detailed implementation of the

fostering process in this format would depend on the context in which the ISC is being fostered.

An ISC is not a single implementation of a concept. Instead, it is multiple implementations of a concept, in different contexts, which together fulfil the overall system's purpose. This existence maps to the nested system characteristic of a GLS, which will be discussed in the next section.

E. General living systems are nested, unitary systems

All living systems consist of similar molecules or components and show an evolutionary progression toward increasing complexity [15]. Essentially what Miller meant by this observation is that all living systems tend to exist as composites of other simpler living systems. Therefore, a living system is a hierarchical suprasystem of its subsystems, which are integrated to form actively self-regulating, developing, unitary systems with purposes and goals [6] [15].

Miller originally identified eight real and concrete hierarchical levels at which hierarchical levels could exist. The eight levels compound as follows: Cells>>Organs>> Organisms>>Groups>>Organizations>>Communities>> Societies>> Supranational. Each new level is more differentiated and considered to be higher than its predecessor; and is composed of all lower-level systems [15]. The vital system components of one level are systems in their own right on the level below. Therefore the larger system is typically the subsystem's environment. The lack of physical cohesion among the components of a living system increases with the level's complexity, but is often compensated for by advanced communication systems which tie the components together [6].

Each level has its typical individual structure and processes. They serve their own purpose which is self-contained while also contributing to the fulfilment of the purpose of the host's larger system. Each system (as discussed in the previous section) takes in inputs that are required selectively for the system's purpose; it then performs its own contextually influenced activities and processes, and outputs products into its environment. The products are then absorbed by another system that selectively requires them for its own throughput processes. This process continues throughout the nested system's levels and hierarchy.

Typically, the literature seems to indicate that organizational culture and its subcultures such as an ISC operate as an overall construct [10]. This construct has been perceived to operate as a solid, single-levelled formal culture. However, the authors do not believe that culture can be considered that simple. Rather, they would like to propose that an ISC is a multileveled composite of nested ISC sub-cultural constructs. Moreover, they would like to propose that a ISC's implementation depends mainly on what business problems are being solved and what the security requirements of that process are, as well as on the business process it surrounds and the stage of the workflow process it is in.

A business process will typically work across multiple departments. Therefore, such a process will circulate throughout parts of the organization's main business process. The business process is therefore a large component of the culture surrounding it. The entire organization has an organizational culture and components of this culture are implemented by some/all of the organization's sub-components, for example departments. Similarly, the ISC, which is also a component of the organizational culture, would have different aspects which are applied in varying degrees within the various departments, because different levels of severity or priority according to the status of the process stage will exist within the specific environment. Cultures are in a sense context-sensitive. Since the ISC is a subculture of the organizational culture, it must sometimes adapt to trade its best practices for secure practices which best facilitate a secure business process in a particular context; these "trade-offs" have always been necessary[4]. Examples of some contextual factors which may necessitate such trade-offs include the role being played by the user or department, as well as the nature, purpose and priorities of the current task being performed [14]. The implementation of an ISC may therefore occur differently within the different departments for their own contributions to the different business processes and their different stages. This may be represented as a nested system of cultures surrounding various work processes which form the artefacts of an ograinsational culture. This is illustrated in Fig. 4.

Fig. 4 illustrates how subcomponents of an ISC can have the same goal, but be implemented separately. This illustration will be further clarified through the use of a real-word ISC example.

Within the example's organizational context, one of the espoused values could be that there must be a strong secure password culture. So the employees in every organizational role are provided with the necessary knowledge (KN) about how to create and manage a password securely. Gradually, the employees develop SAs and AFs which reflect their acceptance and this, in turn, aids the development of a strong, secure password culture. However, what this type of culture is and how it is implemented may be vastly different depending on the particular version of the culture's context.

If System A were the financial department it might have a number of extremely important password-protected work activities. These activities may consist of multiple stages of implementation and, because of their importance within the department, require high security practices to protect their integrity and confidentiality. Therefore, within the financial department a strong, secure password culture would surround this work process. In this example, the password would enable only one employee to access the folder at a time, and they would have to change the password often to prevent unauthorized employees within the department from accessing the information being protected. However, this work process consists of multiple stages and may require input from multiple departments. Therefore, file involved in the process may move to another system, for example ISC System B, which for this example would represent a human resources department. A stage in this work flow process may require multiple employee details as input into its product. However, the secure password culture might differ in this department. It could be that many people in this department need to be able to access the file at any given time. Therefore, in this department all the employees share the password for the process. Moreover, the department

may only define the password as not being secure if someone external to the department knows the password.

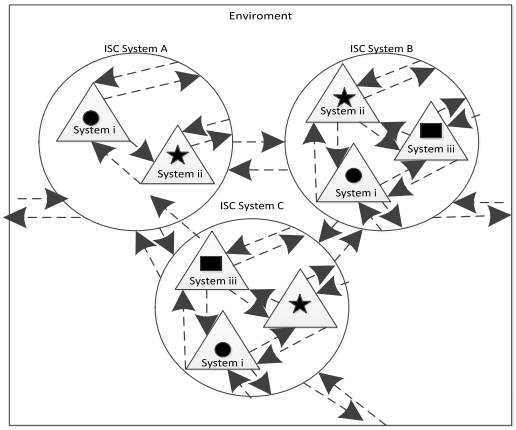


Figure 4: Nested ISCs following a work process

This example is illustrative of a simple scenario. In reality, a scenario may be far more complex, with multiple stages of a process being accessed during a single business workflow, with its importance within the implementation of the ISC varying between systems and even departments.

In summary, an ISC would be very environment and context sensitive. Thus, its visible AFs would differ in accordance the following environmental and system factors: organizational work process, department, priority of process stage within the department, and the department's existing ISC. A living systems view might have many other implications and these will be addressed in future work.

V. Conclusion

This paper has shown that an ISC exhibits, and can be mapped, to five primary characteristics of a general living system. This conceptual mapping indicates that it is possible to conceptually consider an ISC to be a type of general living system. As such it is likely that all/most general propositions associated with all living systems (regardless of size, origin and complexity) are true for ISCs. Therefore, it may be possible to further identify and manipulate the general processes and basic understandings of general systems theory within an ISC. Information security specialists as well as organizational employees may therefore potentially be able to track, monitor and manipulate their ISC based on context-specific occurrences of these GLS prepositions. Lessons learnt from GLS theory could potentially be applied to the fostering and maintenance of ISC. This would also provide tools to further clarify the nature of an ISC. The ability for any employee to understand the ISC as it applies to the *specific* context of his/her own role could be advantageous for the fostering, management and general understanding of the ISC. This general systems theory view of ISC may therefore have implications for all the above-mentioned ISC activities, as well general organizational activities and cultures. Future work will focus on applying such a viewpoint practically in order to evaluate the utility of the GLS view for the purposes of managing an ISC. Additionally, the remaining subsystems of GLS will be mapped to ISC.

References

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

[2] 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.

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

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

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

[6] L. Skyttner, *General Systems Theory: Ideas and Applications*, 2nd Editio. Singapore: World Scientific Printers, 2005, pp. 110–124.

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

[8] “Schlienger and Teufel (2003) Information Security Culture -From Analysis to Change.” .

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

[10] 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.

[11] 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.

[12] 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.

[13] K. Thomson, “Integrating Information Security into Corporate Culture Corporate Culture.”

[14] 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.

[15] J. G. Miller, *Living Systems*. McGraw Hill, 1978.

[16] I. Okere, J. Van Niekerk, and M. Carroll, “Assessing information security culture: A critical analysis of current approaches,” in *Information Security for South Africa (ISSA), Johannesburg, South Africa*, 2012, pp. 1–8.