JISSec
Journal of Information System Security

THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY

Spyridon Samonas
Virginia Commonwealth University, USA

David Coss
Virginia State University, USA

ssamonas@vcu.edu; dcoss@vsu.edu

Journal of Information System Security is a publication of the Information Institute. The JISSec mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

ISSN: 1551-0123
Volume 10, Issue 3

www.jissec.org

Abstract

This paper reviews the history of the CIA (Confidentiality, Integrity and Availability) triad from the perspectives of information security practitioners and scholars. Whilst the former have trusted the technical orientation of the triad as a unique point of reference in information security, the latter have questioned the triad's capacity of addressing the breadth of socio-technical issues that have emerged in security since the 2000s. Through a revisiting of the key tenets of the triad, the paper reconciles these two, seemingly fragmented, approaches. The main argument is that the CIA triad will continue to assume a major role in information security practice. However, this is not due to the fact that practitioners have discarded, or rejected the enhancements that socio-technical security scholars have proposed over the years; rather, it is because these enhancements can be accommodated by a broader re-conceptualization of the original CIA triad. The paper concludes with potential areas for future research.

Keywords: Confidentiality, integrity, availability, socio-technical security

Introduction

For almost 40 years, since the days of the Bell-La Padula and the Biba models, which referred to confidentiality and data integrity respectively (Dhillon and Backhouse, 2001), the terms 'confidentiality', 'integrity' and 'availability' have been widely used in the information security practice and in academic literature. The 'CIA triad', as it

is known, refers originally to the fundamental elements of security controls in information systems. These three key terms have not only shaped and informed our theoretical understanding of information security, but also the very practices through which security is developed and implemented in organizations. Traditionally, these security practices focused on technical controls that protect the confidentiality, integrity, and availability of information. Since the early 1990s, information security scholars have consistently re-assessed the over-reliance on technical controls in light of the socio-technical evolution of the literature on Information Systems (IS), and they have repeatedly stressed the need to account for different non-technical issues in security management. The CIA triad has been criticized on multiple occasions for its narrow technical orientation and focus, and thus, its limited utility when wider organizational and social aspects of security need to be taken into consideration (Anderson, 2002; Dhillon and Backhouse, 2000; Dhillon and Torkzadeh, 2006; Harris, 2002; Kolkowska et al., 2009).

However, information security practitioners still value the symbolic properties of the CIA triad as it provides them with a straightforward way to understand and address problems that relate to information security. The academic literature does not discard the CIA triad, but rather attempts to introduce several enhancements to it. These are mainly in the form of additions of key terms, which essentially expand the scope and utility of the triad to reflect a richer understanding of security management in contemporary organizations. The apparent discrepancy in the views of scholars and practitioners on the evolution and use of the CIA triad qualifies as an oxymoron: Why do practitioners continue to place great confidence in a model that academic literature has deemed largely insufficient? This issue is of particular interest to the authors of this paper, both of whom have worked in the industry as IS practitioners in systems analysis and auditing.

Nevertheless, it is also an issue that is linked to the lag between the academic literature and practice in IS. An assortment of IS scholars have commented on this lag, and have identified a poor state in the relationship between IS literature and practice (Benbasat and Zmud, 1999; Pearson et al., 2005). Based on a bibliographic analysis, Baskerville and Myers (2009) suggest that, whereas the academic literature is aligned with the practitioner literature during fashion upswings, the same does not apply during fashion downswings. In response to this argument, Gill and Bhattacherjee (2009) further note that IS scholars may remain interested in topics that are no longer relevant for practitioners. In the case of the CIA triad, it appears that the proposed enhancements to the triad have not been taken into account by practitioners to develop a revised model.

JISSec
Journal of Information System Security

Drawing on relevant academic and practitioner literature, this paper makes a contribution by bridging the gap between theory and practice. This paper contends that the enhancements put forward by scholars signify a departure from the purely technical origins of the CIA triad and err towards a wider socio-technical reconsideration of its core concepts. A deconstruction and reconstruction of the terms 'confidentiality', 'integrity' and 'availability' can explain sufficiently why practitioners still treat the CIA triad as an emblematic model in information security governance.

The paper is structured as follows. In the following section we provide a historical overview of the CIA triad from its origins as a model for technical controls in security, up until the most recently revised version which appeared in the academic literature in 2011. In the third section we examine some key concepts of the evolution of socio-technical thought in IS security and in the fourth section we re-assess the meaning of each of the components of the CIA triad from a socio-technical perspective. The paper concludes with remarks on the future of the CIA triad and the relationship between IS theory and practice.

The History of the CIA Triad: A practitioner view

During the early days of computers and their usage, there were only a few valid threats to the protection of information. This was primarily due to the fact that computers were expensive, rare and closely safeguarded. The computer systems that contained the information were only exposed to a limited number of people with computing programming skills who had access to the information and could this potentially be a valid threat. Therefore, the initial focus for protecting information was on ensuring the reliability of the system itself, in order to ensure that it would consistently be operable when needed. As a result, information protection was achieved mainly through the control of physical access to computers. As the cost of computer technology decreased, and its usage increased, there was a shift in the focus from the protection of computers to the protection of information. Whereas previously the reliability of computers was dominant, the notion of confidentiality, integrity and availability started to gain importance.

The roots of the CIA triad are deeply entrenched in the military security mindset, which has always been focused on protecting information from external threats. Early on, there was a close link between the practitioner or information security professional, and the academic or information security researcher, with regards to what they believed to be important for the protection of information assets. Many of the initial computer security studies were funded either by federal government or military agencies. Two such studies, the RAND report R-609, Security Controls Systems (The Ware Report, 1970) and the Computer Security Technology Planning

Study (The Anderson Report, 1972), focused on the protection of classified military or government information (Gollmann, 2010). Both of these reports provide extensive classifications of threats to information, however, they primarily concentrate on the protection of information from an external disclosure or a confidentiality point of view. Both the practitioner and academic approaches towards information security evolved from this military/government security view about organizational security, which included additional internal threats. The Anderson Report, which was commissioned by the USAF, identified the following three categories of potential security risks that eventually became the foundation of the CIA triad.

1) Unauthorized information release: an unauthorized person is able to read and take advantage of information stored in the computer. This category of concern sometimes extends to "traffic analysis," in which the intruder only observes the patterns of information use. From those patterns, the intruder can infer some information content. This category also includes the unauthorized use of a proprietary program. (Confidentiality)

2) Unauthorized information modification: an unauthorized person is able to make changes in stored information – a form of sabotage. It should be noted that in the case of this kind of violation, the intruder does not necessarily see the information he has changed. (Integrity)

3) Unauthorized denial of use: an intruder can prevent an authorized user from referring to, or from modifying information, even though the intruder may not be able to refer to, neither modify the information themselves. (Availability)

During this same time period, academic information security researchers began to focus on similar security concerns. Saltzer and Schroeder (1975) in their seminal paper entitled "The Protection of Information in Computer Systems," championed the notion that the primary concern of security should be the protection of the information held inside computer systems, rather than just the protection of the computer system itself. The first section of the paper introduced "basic principles" for the protection of information, which include the triad of confidentiality, integrity and availability.

These types of reports initiated the change in the security mindset, which shifted from protecting computer hardware and software, to protecting the information within them. However, this change began as a slow evolutionary process that focused first on confidentiality, then on integrity, followed by a focus on availability. The most widely adopted early information security models focused primarily on a technical approach to defend against these types of security threats.

The first of these early-adopted models was the Bell-La Padula Model (Bell and La Padula, 1975). This model focused on establishing rules to provide confidentiality and protect information, by limiting access to information objects. Three main rules were enforced: no read up, no write down, and read/write only at same level. These rules were mainly grounded in the military view towards the concept of granting access to information to just to those who "need to know".

The second model that was developed was the Biba Model (Biba, 1975), which focused on data integrity, instead of confidentiality, which was the case of the Bell-La Padula Model. The goals of the Biba Integrity Model are to prevent data modification by unauthorized parties, to prevent unauthorized data modification by authorized parties, and to maintain internal and external data consistency.

The Denning intrusion-detection model focused on defending against threats to availability (Denning, 1987). This model was designed as a real-time intrusion-detection system, which is geared towards the detection of break-ins, penetrations, and other forms of computer abuse. This model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage.

Many of these models were developed in partnerships between government and/or military agencies and academics; however, the acknowledgement of differences between the military and commercial sector led to a change in security goals. In the defense sector the protection of information must be achieved almost at any cost. In the commercial world, the cost of information protection should be balanced with the risk to business. This difference has led to the development and adoption of several security standards and professional certifications. The CIA triad sits at the heart of various security governance standards and codes of practice that have been adopted by public, private and non-governmental organizations over the past 15 years[1]. More specifically, confidentiality, integrity and availability are seen as goals through which information security is achieved (see the ITIL set of practices), but they are also referred to as being an integral part of the expectations that business stakeholders hold for information technology (see the COBIT family of governance frameworks). The loss of confidentiality, integrity and availability of information or information systems is used as a basis for the classification and qualitative assessment of information security risks (see NIST SP 800-30 Rev.1), as well as for the development of relevant security controls (see NIST SP 800-53 Rev.3). Similarly, the CIA triad is also the basis for privacy rules and the protection of electronically-protected health information (see the example of HIPAA in the USA).

[1] In this paper, the BS7799 standard that was released in 1995 by the British Standards Institution is considered a landmark event in information security management, standards, and codes of practice.

Complementing its widespread usage in security governance standards, the CIA triad is featured extensively in the major security, auditing and fraud examination curricula of various professional certification bodies. The scope of the professional certifications that are available can vary significantly, as some of them have a purely technical orientation and focus on computer networks (see the CCNA certification program), whereas others address broader security management or counter-fraud issues (see the ACFE certification). Nevertheless, all these certifications appear to have one thing in common, which is that in their curricula, they treat the confidentiality, integrity and availability of information assets as an indispensable set of controls and principles for security implementation.

CIA triad and beyond: An academic view

Socio-technical aspects of security

Academic research in information and computer security has traditionally adopted a functionalist approach (Dhillon, 2001). This approach has consistently laid emphasis on the technical aspects of security and also the development of controls which focus on the confidentiality, integrity and availability of information and information systems with minimal consideration for the context of use (Hedström et al., 2010). As Dhillon and Backhouse (2001) note, the context for which technical controls, such as the CIA triad, were developed and intended for, is substantially different from that of modern organizations. In an effort to address this shortcoming, security scholars have gradually become more interested in the research that considers wider socio-organizational and socio-behavioral issues of security (Hedström et al., 2010). For instance, significant streams of literature are concerned with security training, education and/or culture (Katsikas, 2000; Vroom & von Solms, 2004), or with various criminological aspects of security breaches (Straub, 1990; Willison and Warkentin, 2013). However, there is still great potential for examining the intersection of security theory and practice, in that much of the literature is still predominantly centered on security policies and standards, as well as on different facets of behavior and compliance (D'Arcy & Greene, 2009).

Socio-technical research advocates that organizations should, ideally, operate on the premise of a harmonious relationship between their technical, social and environmental sub-systems (van Deursen, 2014). Therefore, the importance of socio-technical security research lies in the recognition of the importance of social and human factors in information security management (van Deursen, 2014). Social aspects of security have gradually become an integral part of the IS security literature (Harris, 2010). The very seeds of this evolution can be traced back to the late 1980s. Based on his doctoral research and early seminal work in the field, Baskerville (1988; 1993) stressed the need for alignment between the theory and

practice of IS in the incorporation of security controls and threat-reducing strategies to the logical design of information systems.

Around the same time, Angell and Smithson (1992) adopted a systems-theoretical viewpoint to redefine the concept of risk in organizations and to discuss the social aspects of computer security that were previously systematically ignored in the literature, in favor of the strictly technical aspects of security. They argue that the integrity of the processes that maintain the identity and stability of an organization should be defended at all costs, since the very existence of an organization depends on its 'organizational integrity' – a term which denotes the cohesion, coherence and wholeness of an organization (Angell and Smithson, 1992). Reflecting the systems-theoretical perspective of Angell and Smithson (1992), Dhillon (1995) adopted the TFI (Technical Formal Informal) model (see section below) in his doctoral research to provide a holistic approach to the examination of the socio-technical aspects of security. Drawing on two empirical case studies, Dhillon and Backhouse (1996) argue that failure to achieve a proper balance between the three sub-systems generates uncertainty, creates complexity and also eventually introduces risk. This is due to the continuous and out-of-control interactions of the technical, formal and informal sub-systems (Dhillon and Backhouse, 1996).

As part of the same research agenda on socio-technical security, Dhillon and Backhouse (2000), and Dhillon and Torkzadeh (2006), have pinpointed the limited utility of technical controls and the need for the consideration of social, organizational and managerial aspects of security. To this end, Dhillon and Backhouse (2000) suggested a set of additional principles to the expanded version of the classic CIA triad - which, at that point in time, also included the authenticity (Au) and non-repudiation (nR) of information, as well as the correctness of system specifications (CSpec). More specifically, they argued for the importance of individual Responsibility and knowledge of organizational roles, Integrity as a requirement of organizational membership, and the development of mutual systems of Trust which operate distinctly from controls, as well as a sense of Ethicality which is not derived from rule-following. Dhillon and Kolkowska (2011) further enhanced this RITE framework to incorporate the management of identity at individual and the organization's levels.

The TFI model

For the purpose of re-evaluating the scope of the CIA triad, it is worth examining more closely the continuing contribution of the TFI model, which has been adopted on numerous occasions in socio-technical security studies (Åhlfeldt et al., 2007; Backhouse and Halperin, 2009; Canhoto and Backhouse, 2007; Dhillon, 1995; Dhillon, 2007; Eibl and Schubert, 2008; Halperin, 2006; Samonas, 2012; Spagnoletti

and Resca, 2008). The TFI model represents a conceptual trichotomy of an organization into technical, formal and informal systemic partitions (also referred to as sub-systems) which are in a state of continuous interaction (Åhlfeldt, 2007; Dhillon, 1996). The model is based on the semiotics studies of Stamper (1973) and Liebenau and Backhouse (1990), which are built on the cultural anthropological work of E. T. Hall (1959).

According to Halperin and Backhouse (2007), the three layers of the TFI model, which correspond to three organizational sub-systems, have a mutually constitutive and interdependent relationship, whereby the technical sub-system requires formal organization, and the formal sub-system requires informal organization (Halperin and Backhouse, 2007). In this context, the technical sub-system supports, and is supported by, the formal sub-system, which is actually a bureaucracy that replaces the meanings and intentions of organizational members, with respect to rule and form. These two sub-systems operate within a larger environment 'informal' sub-system, where the meanings and intentions of organizational members are established, understood, altered and discharged. Over time, the 'informal' sub-system is created, which consists of cohesive social groups of organizational members with overlapping memberships in the two aforementioned sub-systems. Some of these social groups can significantly affect the well-being of the organization, as they may well possess enough power to influence other informal groups, or even the formal structures of the organization. From a systemic point of view, the technical, formal, and informal sub-systems all interact with one another in multiple and different ways, which essentially determines and defines 'organizational integrity' (Samonas, 2012).

Drawing on the relevant academic literature and particularly on the application of the TFI model in information security, the next section re-assesses the meaning of each of the terms of the CIA triad, to provide an explanation for its prominence in the practice of security.

Back to the basics: Redefining "CIA"

It is evident in the evolutionary nature of organizational structures, that security controls are subjected to significant modifications, particularly with regards to changing business dynamics (Chowdhuri et al., 2012). To fully grasp this evolutionary process in information security, it is important for academics and practitioners alike to consider how these changes in security controls from the perspective of practitioners can be reconciled with those changes regarding the academic view towards information security. From the 1980s up to the 2010s, eight different terms and concepts have been indicated in the academic literature as being complementary to the CIA triad, namely: authenticity, non-repudiation, correctness

of specification, responsibility, integrity of people, trust, ethicality and identity management. The first two stages of enhancements to the CIA triad can be traced back to the 1980s and 1990s, when practitioners respectively underscored the importance of authenticity and non-repudiation in information management, and also the correctness in the specification of information systems. The remaining two stages were instigated by academics who employed a socio-technical approach to information security (see section 3 of this paper). Table 2 summarizes all the stages that followed the original conception of the CIA triad, along with a legend of the terms and issues that appear in each of the revised definitions of information security over the past 40 years.

In this paper, we argue that even in the 2020s, 50 years after its conception, the CIA triad will still be uniquely relevant for security practitioners and will continue to serve as a point of reference in security management.

Year	Relationships	Legend
1970s	Infosec = CIA	C is Confidentiality, I is Integrity, and A is Availability
1980s	Infosec = CIA + (Au, nR)	Au is Authenticity, and nR is Non-repudiation
1990s	Infosec = CIA + (Au, nR) + CSpec	CSpec is Correctness in Specification
2000s	Infosec = CIA + (Au, nR) + CSpec + RITE +Idn	RITE is Responsibility, Integrity of people, Trust and Ethicality
2010s	Infosec = CIA + (Au, nR) + CSpec + RITE +Idn	Idn is Identity
2020s	Infosec = CIA	

Table 2: Chronological progression of information security issues

Adapted from: Dhillon and Kolkowska (2011)

The use of the terms 'confidentiality', 'integrity' and 'availability' in a broad sense can incorporate any enhancements of the CIA triad – and this is a key reason why practitioners have overlooked subsequent redefinitions of information security and proposed revisions of the triad. To illustrate this, we adopt an etymological

interpretation of each of the three tenets of the CIA triad, and then review them in relation to the eight additional elements that have been discussed over the years in the academic literature. All eight can be classified within one of the tenets (See Figure 1; Confidentiality, Integrity or Availability), or in an intersection between two or more tenets of the CIA triad (see Figure 1; areas 1, 2, 3 or 4). For example, responsibility can be classified as being an element of integrity, and trust can be considered to lie at the intersection of integrity and confidentiality. In certain instances, the exact placement of one of the additional tenets within the original triad may be highly debatable. For instance, we have classified trust as being at the intersection of confidentiality and integrity, whereas other scholars may consider trust to also include aspects of availability (for instance, when individuals or organizations block access to certain websites that are not trusted, and thus impact the availability of information on that site). However, for illustrative purposes, we tentatively allocated all the additional tenets within the triad. Table 3 summarizes the classification of each of the additional tenets that were proposed in the socio-technical security literature into one of the three tenets of the CIA triad.

Additional Tenets	Relation to CIA triad
Authenticity	Integrity
Non-repudiation	Integrity
Correctness in specification	Integrity and Availability
Responsibility	Integrity
Integrity of people	Integrity
Trust	Confidentiality and Integrity
Ethicality	Integrity
Identity management	Confidentiality, Integrity and Availability

Table 3: Classification of additional tenets to the original CIA triad

The remainder of this section will follow a systematic structure as a means to discuss each section of the Venn diagram below (Fig. 1). First the discussion will begin with the review of 'confidentiality' and will then follow a cyclical move through intersection 1, continuing with the review of Integrity, and then moves on to section 2, and so forth.

JISSec
Journal of Information System Security

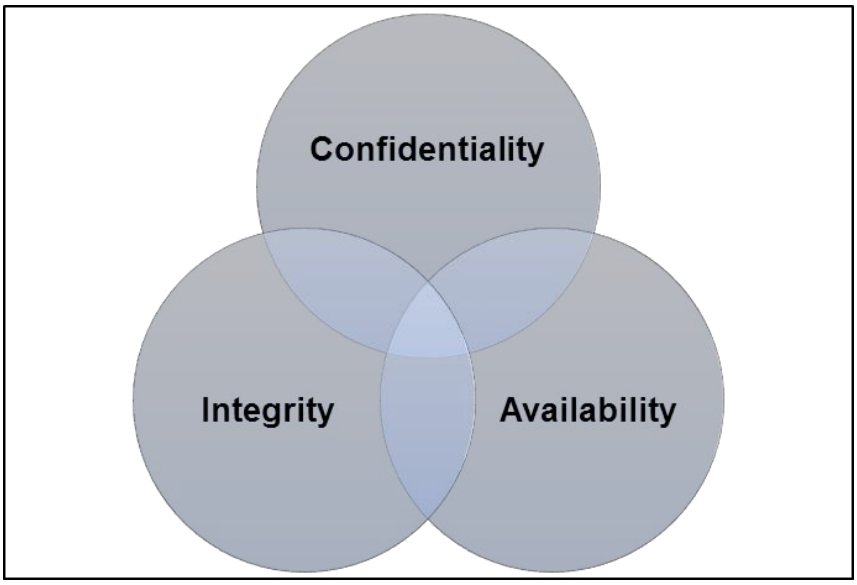

Fig. 1: A revision of the CIA triad

Confidentiality

The term 'confidentiality' is derived from the Latin verb *confidere*, which means "to have full trust or reliance". Confidentiality is a primary tenet of information security which has its roots grounded in the military mindset of maintaining a top down authority and control over those that have access to information, on a need to know basis. Camp (1999) posits that confidentiality implies the notion that data and the information represented by such data must be protected; in such a way that its use is confined to authorized purposes by authorized people only. Similarly, Zwick and Dholakia (2004) define confidentiality as being the perceived ability to carry out an external task which restricts information flow with respect to what is disclosed in it, and to who gets to see it. These aspects of confidentiality are also reflected in official government documents and legislation. For instance, in Section 3542, of Title 44 of the U.S. Code, confidentiality is referred to as the "authorized restriction of information access and disclosure, including the means for protecting personal privacy and proprietary information". Whilst confidentiality has been at the core of information security since the early days of the adoption of information technology, the shifting focus on business needs has downgraded its importance in comparison to other security concerns. Fitzgerald (1995) noted that information confidentiality was no longer a major issue. However he also pointed out that the privacy aspects of confidentiality will grow in importance in the future, particularly in the case of industries where the major business focus is on the management of sensitive personal information - for example, healthcare and finance.

The relation between privacy and trust is an important topic which has been examined in information systems literature from many different perspectives. Katzan (2010) found that an organization's integrity and accountability with respect to their information practices is important for allaying concerns about privacy and for building user trust. Wang, Lee and Wang (1998) argue that the most critical issue identified by Internet customers is fear and distrust with regards to the loss of personal privacy in electronic commerce markets. Researchers who adopt a social exchange theory point of view towards trust, suggest that it is the most important asset on which businesses are built (Luo, 2002; Benassi 1999; Zucker, 1986). The nature and antecedents of trust has been identified as being a major issue for both academic researchers and practitioners (McKnight et al., 2002). We will give more consideration to privacy below in our discussion of intersection 4 (see Fig. 1), which combines all the three elements of the CIA triad.

Section 1 of our Venn diagram is at the intersection of confidentiality and integrity. We have classified the expanded information security element of trust as being within this section. Trust is generally considered to be an inherently ambiguous concept, which is crucial in transactional relationships, especially in the case of those which contain an element of risk (Reichheld and Schefter 2000). Trust may be unconscious or cultivated, and is seen as being necessary as a means of reducing the complexities of life (Luhmann, 1979). Eventually, people have to co-operate in their relationships, and therefore they must trust one another to a certain extent. Trust has been defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other party" (Mayer, Davis, and Schoorman, 1995). Trust has also been described as having three primary forms. Firstly, belief-based trust is an expectation that benevolence exists in others, such as that they will not behave opportunistically by taking advantage of the situation (Cody-Allen & Kishore 2006). Secondly, knowledge-based trust suggests that trust develops over time with the accumulation of relevant knowledge, which in turn results from a certain experience with the other party (Lewicki & Bunker 1995) and accordingly, the development of trust among individual parties requires time and a history of interaction (McKnight et al. 2002). Thirdly, system-based trust is defined as an individual's perception of a system's ability to meet a set of requirements which will lead that individual to believe that the system can be trusted to perform specific tasks (Cody-Allen & Kishore 2006).

Trust entails the investment of responsibility, authority and even resources in others. In the context of security, trust touches upon both confidentiality and integrity. A goal of information integrity is to protect information from

unauthorized modification (Joshi et al., 2001). Information integrity issues are commonly connected with improper storage of information, whereby information is stored in a non-secure manner, which results in a lack of trustworthiness of the stored information, or a lack of a proper authentication control for information access (Wang, Lee and Wang, 1998). Trust is a fundamental property of confidentiality, but it also refers to data access, which can have a significant impact on data integrity, particularly for the perspectives of data accuracy and non-redundancy. Furthermore, trust refers to wider issues of organizational integrity which are raised in the socio-technical studies of security, and are reflected in the informal layer of the TFI model (see Section 3 of this paper). In this respect, the concept of trust as advocated by Dhillon and Backhouse (2001), lies at the intersection of confidentiality and integrity in the CIA triad (see Fig. 1, area 1). The following sub-section will discuss the concept of integrity, as well as the intersection between integrity and availability.

Integrity

From an etymological standpoint, the word 'integrity' means 'soundness', 'wholeness' and it is derived from the Latin word *tangere*, which means 'to touch'. The prefix 'in-' indicates a negative or privative force, and thus the meaning of the word 'integrity' can be associated with certain connotations of the word 'untouchable' - which is, in turn, related to the concept of ethical integrity. In the information security and audit profession, ethicality involves the adherence to commonly accepted principles and values, which are prescribed in the content of various professional standards of practice and qualifications. These professional standards and qualifications are, essentially, verbal agreements between practitioners and their workplace organizations, which outline an assortment of formal and informal responsibilities, as well as certain codes of conduct with regards to information security. In this respect, the issues of ethicality and responsibility, which are seen as being key principles of security and are enhancements to the CIA triad (Dhillon and Backhouse, 2001), both fall under a wider conceptualization of 'integrity'.

Ethics has been described as being a process, which involves systematizing, defending, and recommending concepts of right and wrong behavior (Fieser, 2006). Information security research has studied ethics from many different points of view. Gattiker and Kelley (1999) studied differences in users' attitudes and moral judgments with regards to ethical computer-related behavior. Cardinali (1995) suggests that state and federal legislation be used as safeguards against unethical behavior. Along similar lines, Harrington (1996) recommends that the enforcement of codes and policies, and the communication of sanctions can be swiftly dispensed to defaulting personnel. Sipior et al. (2005) argue that training and awareness of

computer security is one way to defend against unethical behaviors. A strong argument has been made in the literature that management should set the appropriate tone for the organization, and that it should motivate employees (Bowen, 2004) to do the right thing, and to be resolved to not do the wrong thing.

Structures of responsibility should provide a means for understanding the manner in which responsible agents are identified, and also: the formal and informal environments in which they exist; the influences they are subjected to; the range of conduct open to them; the manner in which they signify the occurrence of events; the communications they enter into, and above all; the underlying patterns of behavior (Backhouse and Dhillon, 1996). Formal responsibility arises in relation to the requirements that are established in job descriptions, whereas informal responsibility encompasses the need of dedicated employees to protect their workplace organization against insider and outsider threats (Williams, 2008). In this context, and with reference to the ethical connotations of the word, integrity refers to not only the ethical behavior of employees, but also to the responsibilities that emanate from their job roles and their active participation in an organization.

In a more technical definition of integrity, Section 3542 of Title 44 of the U.S. Code defines integrity as being the prevention of "improper information modification or destruction", and specifically includes information authenticity and non-repudiation (von Solms, 2013). In the latter part of the definition, authenticity and non-repudiation are two very closely related security terms. More specifically, authenticity does not guarantee non-repudiation, however non-repudiation guarantees authenticity. Non-repudiation involves the inability to defy a certain transaction or to communication between two parties, which implies that an adequate authentication[2] process has successfully taken place in the first instance. Authenticity denotes the quality of being original and genuine, and therefore authentication is the process of verifying, to some desired level of confidence, that a claimed identifier is valid and is actually associated with a particular item or person.

Section 2 of our Venn diagram is at the intersection of integrity and availability. We have included the expanded information security element of correctness of specifications as being within this section. In the former part of the technical definition, integrity refers to the assurance that data will not be altered without appropriate authorization. This is where the correctness of specifications becomes relevant, as it ensures that the system is fit for purpose, according to the requirements that are established by the various stakeholders, such as owners and users. Besides its more technical aspects, where logical reasoning and formal

[2] For the purposes of our analysis, the words 'authenticity' and 'authentication' are used interchangeably throughout this paper, unless stated otherwise.

mathematical methods are applied to validate and verify the design of the system, the correctness of specifications also demonstrates elements of a socio-technical process. It relates to the basic definition of 'integrity' as being 'wholeness', which was presented at the very beginning of the current sub-section, and correct specifications lay the foundations for robust and coherent access control, which is directly related to the availability of data. The way in which access control to the data is structured and enforced affects the usability of a system and sometimes this creates a tension between security and usability, which has been discussed in the security literature on multiple occasions (Dhamija and Dusseault, 2008; Choobineh et al., 2007). Due to its richness and significance in the development of information systems, the correctness of specifications is not solely an issue that is related to integrity, but rather it falls in the intersection between integrity and availability (see Fig. 1, area 2). The final sub-section will discuss the concept of availability and the remaining intersections between the other tenets of the CIA triad.

Availability

The word 'availability' comes from the Latin *valere*, which means to 'be worth'. In information security, the term availability means "timely and reliable access and use of information" (44 USC Sec. 3542). This entails the aspects of access which were mentioned in the previous sub-section of this paper, and which will also be covered in the next sub-section, under identity management, as well as aspects that pertain to the usability of systems. From a usability engineering perspective, a system is considered usable when it is effective and efficient, and its users are generally satisfied with its performance of specific tasks within a certain environment (Weir et al., 2009). In the case of security software, Padayachee (2012) cites Whitten and Tygar (1999) in noting that usability is also associated with the capacity to avoid dangerous errors and to make users reliably aware of the tasks they need to perform.

The relationship between usability and security can be best described as strenuous[3]. The security literature has discussed extensively the conflict between security and usability with regards to different aspects of authentication, such as password mechanisms (Weir, 2009), and single-factor and two-factor authentication solutions (Gunson et al., 2011). Empirical research indicates that users typically choose usability and convenience instead of security (Weir, 2009; Gunson et al., 2011). However, despite several calls to address this conflict, there are very few theoretical approaches, which offer a balanced approach to the development of security and usability (Dhillon et al., 2012). Ultimately, usability is linked to

[3] In this paper, we focus on the relationship between system usability and security. However, similar conclusions have been drawn in the literature with regards to the relationship between convenience and security (Chapman, 2012; Dhillon et al., 2012)

productivity through security. A heavy investment in information security can result in lower usability, and therefore a loss in productivity, which can, in turn, have an adverse effect on the business (Cowan, 2012). As Cowan notes (2012), usability is a battle between security and productivity, as security measures can neither be so restrictive that they affect business processes and the flow of information, nor too relaxed, thereby causing harm.

Section 3 of our Venn diagram is at the intersection of availability and confidentiality. For this intersection we have not classified any of the CIA extension terms as being within the section. We believe that this is primarily due the emphasis on maintaining the integrity of the data and information that reside in the system. However, we believe that this is an area ripe for research in the coming years, on account of the increase of mobile technologies and privacy concerns.

The evolution of information systems has resulted in an amalgamation of various technologies to meet the demands of global organizations. This expanding complexity within technology environments necessitates stronger identity management controls (Gopalakrishman, 2009). We consider identity management to lie at the center of intersection 4, and to be equally influenced by all of the three CIA tenets. Identity management has been broadly defined as being the management of digital identities or personal identifying data (Halperin and Backhouse, 2008). Identity management has also been identified as one of the core components for ensuring cloud privacy and security (Coss, 2013). Historically, identity management has been viewed through a technical lens with a focus on confidentiality and availability through its emphasis on authentication and authorization protocols (Sandhu and Buell, 2003). IS researchers have suggested that technical controls, such as digital signatures for non-repudiation, cryptography strategies for encrypting databases and data transfers or federated identity management systems, are the best solutions for managing individuals' identities (Yan, Rong, Zhao, 2009; Jensen, et al. 2009). While this area continues to pose many challenges for security architects and designers, there has been a renewed focus on identity management, as it is related to the protection and integrity of personal identification information from a more formal and informal perspective.

Formal controls are needed to protect and ensure the entire lifecycle of user identities and also their associated credentials and entitlements (Gopalakrishman, 2009). Without better controls for managing identities, we will continue to struggle with issues such as identity theft, spam, malware, and cyber fraud, and we will also be unable to ensure individual users that their privacy is protected (Cavoukian, 2009). Angin et al. (2010) argue that there is a strong need for an efficient and effective privacy-preserving system for managing personal identifying information.

Dinev et al. (2013) share this sentiment and suggest that "when confidentiality is assured by preventing unauthorized access, consumers may perceive higher levels of control over their personal information". We consider privacy to be linked to the core of the security and the CIA triad, through aspects of identity management controls. Halperin and Backhouse (2008) posit that the relations between security and privacy are at the forefront of the identity discourse in the emerging information society. Privacy and security are on the opposite sides of the scale, and thereby the presence of more of one, implies less of the other. For example, in the name of fighting terrorism or cyber security, governments collect personal information about the private activities of their citizens. When unauthorized access is given to unscrupulous individuals, the integrity of the entire system is at risk, not only for the company itself, but also for all of its customers who have their personal information stored within the compromised system.

Conclusion

This paper has reviewed the conception and use of the CIA triad from two, seemingly fragmented, approaches to information security. Firstly, we looked at the way in which practitioners have been consistently portraying the triad as a unique point of reference in information security. Secondly, we examined how academic research in information systems security has suggested several socio-technical extensions to the original CIA triad, in order to address the limited scope of technical controls. Our goal was to provide a plausible explanation as to why security practitioners have largely ignored these extensions and continue to place great importance in the key components of the CIA triad itself. To this end, we presented a redefinition of the triad in a manner which essentially incorporates all the different socio-technical extensions, and thereby reconciles the two standpoints. A closer look at the major professional certification curricula and standards of practice in security indicates that practitioners have not refuted the utility and value of the academic perspective. Conversely, they use the triad under an expanded meaning, which goes beyond the strictly technical aspects of the original conceptualization of CIA. Despite the lag in the alignment of different approaches, there seems to be an ongoing dialogue whereby academic research informs standards of practice, whilst practitioner norms and insights inform the view of security scholars. Over the course of more than 40 years of history, the CIA triad has undergone a quiet process of reinvention and reconfiguration, in order to accommodate the exponential growth of information technology and the significant changes in views toward security – evolving from the initial focus, through to data shifting of information, and lately to cyber security.

Throughout our analysis we noticed a lack of research interest in the area intersected by availability and confidentiality. It appears that the majority of the CIA expansion concepts are focused just on protecting the integrity of data that resides in a system. On account of the increased usage of mobile technologies, combined with the growing concern about privacy, we believe that in future expansions of the CIA triad that the intersection of availability and confidentiality will offer a more fashionable agenda for information security researchers to study further. An additional avenue for future researchers is to explore the relationship between security and privacy, which addresses a variety of social implications and questions, which still need to be resolved. Our future research agenda is concentrated on understanding how security practices vary across different industries with respect to the application of CIA and the extension of its concepts. We are also interested as to whether the gap between current information security practices and the academic research agenda is, in fact, narrowing. One aspect of this research is that, as technology evolves and different types of technology-in-use come into management fashion, then different aspects of the CIA triad will be more dominant than others, as was the case in the past.

References

Åhlfeldt, R.-M., Spagnoletti, P. and Sindre, G. (2007). Improving the Information Security Model by using TFI, In *IFIP International Federation for Information Processing Proceedings, Vol. 232, No. 1: New Approaches for Security, Privacy and Trust in Complex Environments*, Springer, pp. 73-84.

Anderson, J. (2002). Why we need a new definition of information security. *Computer & Security*, 22 (4), 308-313.

Angin, P., Bhargava, B., Ranchal, R., Singh, N., Othmane, L.B., Lilien, L. and Linderman, M. (2010). An Entity-centric Approach for Privacy and Identity Management in Cloud Computing, 29th IEEE Symposium on Reliable Distributed Systems, Oct 31-Nov 3 New Delhi, India.

Backhouse, J. and Halperin, R. (2009). *Approaching interoperability for identity management systems,* Springer.

Baskerville, R. (1988). *Designing information systems security,* Wiley, Chichester England; New York.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development, *ACM Computing Surveys (CSUR),* **25**, 4, 375-414.

Baskerville, R. L., & Myers, M. D. (2009). Fashion waves in information systems research and practice. *MIS Quarterly*, 33(4), 3.

Benassi P. (1999). TRUSTe: an online privacy seal program. *Communications of the ACM* Volume 42 Issue 2, Feb. 1999, 56 – 59.

Benbasat, I., & Zmud, R. W. (1999). Empirical research in information systems: the practice of relevance. *MIS Quarterly*, 3-16.

Bell, D., and La Padula, L. (1975). Secure Computer System: Unified Exposition and Multics interpretation. Technical Report ESD-TR-75-306, The MITRE Corporation, Bedford, MA.

Biba, K.J. (1975). Integrity Considerations for Secure Computer Systems. Technical Report MTR-3153, MITRE Corporation, Bedford, MA.

Bowen, S. A. (2004). Organizational Factors Encouraging Ethical Decision Making: An exploration into the case of an exemplar. *Journal of Business Ethics* 52(4), 311-324.

Camp, L. J. (1999). Web security and privacy: An American perspective. *The Information Society*, 15(4), 249-256.

Canhoto, A. I. and Backhouse, J. (2007). Profiling under conditions of ambiguity—An application in the financial services industry, *Journal of Retailing and Consumer Services,* **14**, 6, 408-419.

Cardinali, R. (1995). Reinforcing our moral vision: Examining the relationship between unethical behavior and computer crime. Work Study 44(8), 11-17.

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada

Chapman, M. (2012). In *Information security management handbook*, (Eds, Tipton, H. F. and Krause, M.), CRC Press.

Choobineh, J., Dhillon, G., Grimaila, M. R. and Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems,* **20**, 1, 57.

Chowdhuri, R., Dhillon, G., & Harris, M. A. (2012). Understanding Information Security. *Journal of Information System Security*, 8(2).

Cody-Allen E., Kishore R. (2006). An Extension of the UTAUT Model with E-Quality, Trust, and Satisfaction Constructs, Proceedings of the SIGMIS conference, April 13-15, Claremont, CA, USA, ACM Press, 82-89

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems*, 20(1), 57.

Coss, D. L. (2013). Cloud Privacy Audit Framework: A Value-Based Design (Doctoral dissertation, Virginia Commonwealth University, Richmond, Virginia).

Cowan, D. (2012). Comment: Too Much Security May Affect Business Processes, Infosecurity, 27 June 2012, http://www.infosecurity-magazine.com/view/26550/ comment-too-much-security-may-affect-business-processes/, last accessed on 16th July 2014.

D'Arcy, J. & Greene, G. (2009). The multifaceted nature of security culture and its influence on end user behavior. In International Workshop on Information Systems Security Research (pp. 145-157).

Denning, D. E. (1987). An intrusion-detection model. Software Engineering, IEEE Transactions on, (2), 222-232.

Dhamija, R., & Dusseault, L. (2008). The seven flaws of identity management: Usability and security challenges. *IEEE Security & Privacy*, 6(2), 24-29.

Dhillon, G. (1995). *Interpreting the management of information systems security,* Department of Information Systems, The London School of Economics and Political Science (LSE), London, UK.

Dhillon, G. (2001). *Information security management: Global challenges in the new millennium,* Idea Group Publishing, London, UK.

Dhillon, G. (2007). *Principles of information systems security: text and cases,* John Wiley & Sons, Hoboken, NJ.

Dhillon, G. and Backhouse, J. (1996). Risks in the use of information technology within organizations, *International Journal of Information Management,* **16**, 1, 65-74.

Dhillon, G. and Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium, *Communications of the ACM,* **43**, 7, 125-128.

Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives, *Information Systems Journal,* **11**, 2, 127-153.

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2012). When Convenience Trumps Security: Defining Objectives for Security and Usability of Systems. In Information Security and Privacy Research (pp. 352-363). Springer Berlin Heidelberg.

Dhillon, G. and Kolkowska, E. (2011). Can a cloud be really secure? A socratic dialogue, In *Computers, privacy and data protection: an element of choice*, Springer, pp. 345-360.

Dhillon, G. and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal,* **16**, 3, 293-314.

Dinev, T., Xu, H., Smith, J. H., and Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295-316.

Eibl, C. J. and Schubert, S. E. (2008). Development of e-learning design criteria with secure realization concepts, In *Informatics Education-Supporting Computational* Thinking, Springer, pp. 327-336.

Fieser, James, Ethics, The Internet Encyclopedia of Philosophy (2006), at www.iep.utm.edu/ (accessed on 30 December 21, 2014).

Fitzgerald, K. J. (1995). Information security baselines. *Information Management & Computer Security*, 3(2), 8-12.

Gattiker, U.E. and H. Kelley: 1999, Morality and computers: Attitudes and differences in judgments, *Information Research*, 10(3); p. 233

Gill, G., & Bhattacherjee, A. (2009). Whom are we informing? Issues and recommendations for MIS research from an informing science perspective. *MIS Quarterly*, 33(2), 3.

Gollmann, D. (2010). Computer security. Wiley Interdisciplinary Reviews: Computational Statistics, 2(5), 544-554.

Gopalakrishnan, A. (2009). Cloud computing identity management. *SETLabs briefings*, 7(7), 45-54.

Gunson, N., Marshall, D., Morton, H. and Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking, *Computers & Security,* **30**, 4, pp. 208-220.

Hall, E. T. (1969). The silent language. 1959. Hidden Dimension.

Halperin, R. (2006). Identity as an emerging field of study, *Datenschutz und Datensicherheit - DuD,* **30**, 9, 533-537.

Halperin, R., & Backhouse, J. (2007). Using structuration theory in IS research: Operationalizing key constructs. Proceedings of the International Conference on Information Systems, (ICIS), p127.

Halperin, R., & Backhouse, J. (2008). A roadmap for research on identity in the information society. *Identity in the information society*, 1(1), 71-87.

Harrington, S. J. (1996), The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly* 20(3), 257-278.

Harris, S. (2002). CISSP all-in-one certification exam guide. New York, USA: McGraw-Hill/Osborne.

Harris, M. (2010). The Shaping of Managers' Security Objectives Through Information Security Awareness Training, Department of Information Systems, Virginia Commonwealth University, Richmond, Virginia, USA.

Hedström, K., Dhillon, G., & Karlsson, F. (2010). Using actor network theory to understand information security management. In Security and Privacy–Silver Linings in the Cloud (pp. 43-54). Springer Berlin Heidelberg.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On technical security issues in cloud computing. In *Cloud Computing*, 2009. CLOUD'09. IEEE International Conference on (pp. 109-116). IEEE.

Joshi, J. B., Aref, W. G., Ghafoor, A., & Spafford, E. H. (2001). Security models for web-based applications. *Communications of the ACM*, 44(2), 38-44.

Katsikas, S. (2000). Health care management and information systems security: awareness, training or education? *International Journal of Medical Informatics*, 60(2), 129-135.

Katzan Jr, H. (2011). On the privacy of cloud computing. *International Journal of Management & Information Systems*,14(2).

Kolkowska, E., Hedström, K., & Karlsson, F. (2009). Information security goals in a Swedish hospital. In Security, assurance and privacy: organizational challenges. 8th Annual Security Conference, 15-16 April 2009, Las Vegas, USA.

Lewick, R. J., & Bunker, B. B. (1996). Developing and maintaining trust in work relationships. Trust in Organizations: Frontiers of Theory and Reach, 114-39.

Liebenau, J. and Backhouse, J. (1990). *Understanding information: an introduction,* Macmillan, London.

Luhmann, N. (1979). Trust and Power. Chichester: Wiley.

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. Industrial Marketing Management, 31(2), 111-118.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of management review, 709-734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334-359.

Olden, M. and Za, S. (2010). Biometric authentication and authorization infrastructures in trusted intra-organizational relationships, In *Management of the Interconnected World*, Springer, pp. 53-60.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, 31(5), 673-680.

Pearson, J. M., Pearson, A., and Shim, J. P. (2005). The Relevancy of Information Systems Research: The Practitioner's View. *Information Resources Management Journal* (18:3), pp. 50-67.

Reichheld, F. F., Schefter, P., (2000). E-Loyalty: Your Secret Weapon on the Web, *Harvard Business Review*, 78 4 105.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(9), 1278-1308.

Sandhu, R., & Buell, D. A. (2003). Guest Editors' Introduction: Identity Management. *IEEE Internet Computing*, 7(6), 0026-28.

Samonas, S. (2012). *Managing Computerized Bureaucracy: Opportunities and Hazards,* Department of Management, Information Systems and Innovation Group, London School of Economics and Political Science (LSE), London, UK.

Sipior, J. C., B. T. Ward and G. R. Roselli (2005). The Ethical and Legal Concerns of Spyware. *Information Management* 22(2), 39-49.

Smithson, S. and Angell, I. (1991). *Information systems management: opportunities and risks,* Palgrave Macmillan.

Spagnoletti, P. and Resca, A. (2008) The duality of Information Security Management: fighting against predictable and unpredictable threats, *Journal of Information System Security,* 446-62.

Stamper, R. (1973). Information in business and administrative systems. John Wiley & Sons, Inc.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276.

van Deursen, N. (2014). *HI-Risk: a Socio-Technical Method for the Identification and Monitoring of Healthcare Information Security Risks in the Information Society,* Institute for Informatics and Digital Innovation, Edinburgh Napier University, Edinburgh, UK.

von Solms, R. and van Niekerk, J. (2013). From information security to cyber security, *Computers & Security,* **38**, pp. 97-102.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191-198.

Wang, H, Lee, M, and Wang, C. (1998). Consumer Privacy Concerns about Internet Marketing. *Communications of the ACM*, March 1998, Volume 41, Number 3, 63-70.

Weir, C. S., Douglas, G., Carruthers, M. and Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens, *Computers & Security,* **28**, 1-2, pp. 47-62.

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Usenix Security (August).

Williams, P. A. (2008). In a 'trusting' environment, everyone is responsible for information security. Information Security Technical Report, 13(4), 207-215.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20.

Yan, L., Rong, C., & Zhao, G. (2009). Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. *Cloud Computing*, 167-177.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. *Research in Organizational Behavior*, Vol 8, 1986, 53-111.

Zwick, D., & Dholakia, N. (2004). Whose identity is it anyway? Consumer representation in the age of database marketing. *Journal of Macromarketing*, 24(1), 31-43.