Understanding Information Assurance and Security

Yulia Cherdantseva[a,1], Jeremy Hilton[b]

[a]*School of Computer Science and Informatics, Cardiff University, Queen's Buildings, 5 The Parade, Roath, Cardiff CF24 3AA, UK. Email: y.v.cherdantseva@cs.cardiff.ac.uk, Tel: +44 (0)29 2087 4812, Fax: +44 (0)29 2087 4598*

[b]*Department of Informatics and Systems Engineering, Cranfield University, Shrivenham, Swindon, UK. Email: j.c.hilton@cranfield.ac.uk, Tel: +44 (0) 1793 785733*

Abstract

Despite great interest of researchers and professionals in Information Security (InfoSec) and Information Assurance (IA), there is still no commonly agreed understanding of the disciplines. The paper aims to clarify the meaning, scope and goals of InfoSec and IA as well as the relationship between the disciplines. Clarity of the scope and goals of InfoSec and IA is important because this knowledge serves as a foundation for the definition of (1) curricula for the InfoSec and IA education programs, (2) responsibilities of practitioners, and (3) organisations' InfoSec strategy and policies. The study analyses US and European InfoSec- and IA-related official publications and standards, and discusses the perception of the disciplines in academic and industry works. The study highlights the importance of clear and precise definitions of InfoSec and IA, and a need for the definitions to promote open-mindedness among practitioners and researchers. Since the existing definitions of InfoSec and IA do not fully reflect the complexity and the evolving nature of the disciplines, the contemporary adapted definitions of InfoSec and IA are elaborated in the paper.

[☆]This manuscript is a draft of Chapter 2 of the PhD thesis: Cherdantseva, Y.: "Secure*BPMN - a graphical extension for BPMN 2.0 based on a Reference Model of Information Assurance & Security", PhD THESIS. CARDIFF UNIVERSITY. UK. 2014. The full text of the thesis is available at ORCA: http://orca.cf.ac.uk/74432. This material is also presented in Cherdantseva Y. and Hilton J. "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals, In: F. Almeida, and I. Portela (eds.), Organizational, Legal, and Technological Dimensions of IS Administrator. IGI Global Publishing. September, 2014. Full text is available at http://www.igi-global.com/chapter/information-security-and-information-assurance/80717.

Keywords: Information Security, Information Assurance, definition, scope, goals, Computer Security

---

"The beginning of wisdom is the definition of terms."
Socrates

1. Introduction

Information Security (InfoSec) and Information Assurance (IA) have become increasingly important in an era in which information is recognised as a key asset by many organisations. The rapid advancement of Information and Communication Technology (ICT) and the growing dependence of organisations on IT infrastructure continuously intensify the interest in these two disciplines. Organisations pay increasing attention to information protection also because the impact of security breaches today have a more tangible, often devastating effect on business (Dlamini et al., 2009).

The number and severity of security breaches grows. In 2007, the TJX Company lost, according to different sources, from 36.2 to 94 million customers' credit and debit cards records (Shaw, 2010). In 2011, Sony reported a data breach that had resulted in the loss of personal details of 77 million customers (Sony, 2011). According to the *Information Security Breaches Survey 2010* (PwC, 2010), the number of large companies in the UK that suffered a security incident during 2010 increased up to 92%, in comparison to 72% in 2008. The average cost of the worst security incident in large UK companies increased from £170,000 to £690,000. In the US, the number of security breaches detected by law enforcement increased up to 33% in 2011, against 7% in 2010 (Trustwave, 2012).The spending on InfoSec worldwide stayed stable in 2011 (ISC, 2011), even despite the economic downturn. In 2012, security budgets received higher priority worldwide compared with 2011 (Gartner, 2012). Gartner predicts a stable (at the annual rate of 9%) growth of security market until 2016. As a result, the spending on security is expected to grow from $55 billion in 2011 to $86 billion in 2016 (Gartner, 2012).

In response to the growing interest, a significant amount of research has been conducted over the past two decades to cover various perspectives of InfoSec and IA: the technical side (Anderson, 2001a); the human factor

(Lacey, 2009); the business and economic perspectives (Pipkin, 2000; Anderson, 2001b; Sherwood et al., 2005); and the governance (SANS, 2004; FRC, 2004; Sherwood et al., 2005). Despite great interest in InfoSec and IA, there is still no commonly agreed understanding of the disciplines. Every author makes a unique interpretation of InfoSec and IA by identifying the divergent scopes and goals of the disciplines. The approaches to InfoSec and IA vary, depending on the background of an author and on the nature of an author's occupation. InfoSec and IA remain open to diverse interpretations, partly due to the fact that both disciplines are inevitably evolving. Many studies highlight continual changes of InfoSec (Parker, 1998; Pipkin, 2000; Anderson, 2001a; Lacey, 2009; ISACA, 2009). Therefore, a revision of the meaning, scope and goals of the disciplines has to be conducted periodically to reflect this fluctuating environment.

The motivation of this study stems largely from the lack of a consistent, clear approach to InfoSec and IA, and, furthermore, from the existing misinterpretations of the terms. Despite the fact that both, InfoSec and IA, have been intensively discussed, there are still no commonly accepted definitions of the terms. The relationship between InfoSec and IA remain disputable. This study also originates from the necessity to resolve the controversy within InfoSec and IA concerning the overall goals and the scope of the disciplines. This paper analyses different approaches to InfoSec and IA in order to draw a state-of-the-art picture of the disciplines in the permanently changing landscape.

The main objectives of this study are, first, to outline the up-to-date and precise realms of InfoSec and IA and, second, to develop an adapted refined definition of each discipline in light of these findings. The paper aims to answer the following questions:

- What is Information Security: its meaning, scope and main goals?
- What is Information Assurance: its meaning, scope and main goals?
- What are the differences, similarities and relationship between the disciplines?

The clarity and unambiguity of the scope and goals of InfoSec and IA are important because this knowledge serves as a foundation for the definition of (1) curricula for the InfoSec and IA education programs, (2) responsibilities of practitioners, and (3) organisations' InfoSec strategy and policies. Hence,

the discussion may also be seen as answering the question about what an InfoSec or IA expert should be taught and what s/he should be responsible for in an organisation.

The conventions used in the study are explained below. The members of the classic information security triad - confidentiality, integrity and availability (also referred to as the CIA-triad) - are interchangeably referred to in the literature as security attributes, properties (CSIA, 2007; CNSS, 2010), goals (NIST, 2002), fundamental aspects (Pipkin, 2000), information criteria (ITGI, 2007), critical information characteristics (McCumber, 1991) and basic building blocks (Pipkin, 2000). In order to highlight the fact that these are the *desirable* properties of information (or *desirable* abilities of information systems, where appropriate), in this paper the term *security goal* will be applied to refer to confidentiality, integrity, availability, non-repudiation, accountability, reliability and the like. In this study we will also distinguish between a *security goal* and a *security mechanism*, which is defined as an established process by which certain security goals are achieved. This work does not aim to provide a detailed analysis of security goals. Nevertheless, security goals are discussed to the extent required to answer the research questions.

The rest of the paper is structured as follows. Sections 2 and 3 provide a detailed overview of InfoSec and IA respectively. In order to draw a clear image of the present state of the disciplines, for each discipline (1) a general perception of the term is discussed, (2) the interpretations of the term in the official standards and publications are analysed, and (3) the understanding of the term in related academic and industry publications is overviewed. Section 4 outlines the comparison of InfoSec and IA and formalises the relationship between the disciplines. In Section 5, we present the adapted definitions of InfoSec and IA. Section 6 draws some conclusions and illustrates the benefits of the study.

2. Information Security

This section contains a detailed analysis of the term InfoSec. First, an analysis of the term based on common English is conducted. Second, the definitions of the term as suggested in the official standards are discussed. Third, the understanding of InfoSec in academic and industry publications is researched, and the latest trends in InfoSec are distilled. Finally, an adapted contemporary definition of InfoSec is presented and discussed.

2.1. The Definition of Information Security based on common English

Formal or academic definitions are often distinct from the common comprehension of terms (Neumann, 1995; Parker, 1998). In order to understand the common perception of the term InfoSec we start from the definitions of isolated words *information* and *security* in the Collins English Dictionary (2012) (the definitions are abridged):

- Information n.
    1. knowledge acquired through experience or study;
    2. computing
        a. the meaning given to data by the way in which it is interpreted
        b. another word for data.

- Security n.
    1. the state of being secure;
    2. precautions taken to ensure against theft, espionage, etc.

Secure is defined as *"free from danger, damage, etc; not likely to fail; able to be relied on"* (Collins English Dictionary, 2012). Precaution is defined as *"an action taken in advance to prevent an undesirable event"* (Collins English Dictionary, 2012). The Oxford English Dictionary (2012), in turn, defines security as *"the state of being free from danger or threat"*. Based on the above, a general definition of InfoSec could be derived:

Information Security is a discipline, the main aim of which is to keep the knowledge, data and its meaning free from undesirable events, such as theft, espionage, damage, threat and other danger. Information Security includes all actions, taken in advance, to prevent undesirable events happening to the knowledge, data and its meaning so that the knowledge, data and its meaning could be relied on.

In the general definition of InfoSec five points should be highlighted. First, there are no restrictions on the information type. In the broad sense, InfoSec is concerned with information of any form or type (e.g. electronic, paper, verbal, visual). Second, InfoSec includes *all* actions to protect information. Thus, InfoSec is concerned not only with technical actions, but deals with the full diversity of protecting actions required during information processing, storage or transmission. Third, the list of undesirable events is broad and open. The definition explicitly lists theft, espionage and damage of the

information, but is not restricted to them. Thus, InfoSec deals with the protection of information from *all* undesirable events. Fourth, the general definition of InfoSec does not state any security goals such as confidentiality, integrity, availability or any other. Therefore, in line with the third point, the main aim of the discipline is the overall protection of information, and not just the achievement of several pre-defined security goals. Fifth, InfoSec includes actions taken *in advance*. Therefore, InfoSec should be concerned not only with an analysis of undesirable events, which have already taken place, but also with the anticipation of such events and an assessment of the their likelihood.

2.2. Information Security as defined in the official documents

There is a plethora of standards covering the various aspects of InfoSec published by international organisations (ISO, IEC, ITU), national standards bodies (BSI, NIST, SAA, SNZ, JISC), non-profit organisations (ISACA, ANSI, IEEE, OMG, OASIS, ETSI) and international communities (IETF, W3C, EEMA, Wi-Fi Alliance, ISF).

In this section the definitions of InfoSec provided in the vocabulary of the ISO/IEC 27000 series (ISO27000, 2009) and in the National Information Assurance Glossary (CNSS, 2010) are analysed, and compared to the definition suggested by ISACA (ISACA, 2008).

The ISO/IEC 27000 series of standards is an internationally recognised and widely adopted InfoSec standard. The series was developed by a joint committee of the International Organisation for Standardisation (ISO) and the International Electronic Commissions (IEC) and covers InfoSec management, InfoSec risk management, implementation of InfoSec Management Systems (ISMS), measurements and metrics of ISMS. In 2000, the ISO adopted BS7799, the standards published by the British Standard Institute in 1995, under the name ISO/IEC 17799. BS7799 was based on the Code of Practice for Information Security Management, which was developed by the Department of Trade and Industry in close rapport with leading UK organisations. In 2007, ISO/IEC 17799 was incorporated in the ISO/IEC 27000 series as ISO/IEC 27002.

The National Information Assurance Glossary, published by the Committee on National Security Systems (CNSS), is also known as the CNSS Instruction 4009 (CNSSI) (CNSS, 2010). The glossary was created to resolve the differences between the definitions of terms used by the U.S. Department of Defense (DoD), Intelligence Community and National Institute of

Standards and Technology Glossary (NIST). NIST develops U.S. Federal Information Processing Standards publications (FIPS PUB). The standards are primarily oriented on the government systems, but are also useful for industry.

ISACA is a non-profit, global association of over 95,000 members worldwide. It develops practices for information systems. ISACA is an originator of the globally accepted Control Objectives for Information and related Technology (COBIT) framework.

The definitions of InfoSec suggested in the three documents mentioned above are summarised in Table 1, along with the definitions of integrity, which are discussed later in this section.

Table 1: Definitions of Information Security and Integrity

Term Standard	Information Security	Integrity
ISO27000 (2009)	Preservation of confidentiality, integrity and availability of information. Note In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.	The property of protecting the accuracy and completeness of assets.
CNSS (2010)	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	The property whereby an entity has not been modified in an unauthorized manner.
ISACA (2008)	Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability).	The accuracy, completeness and validity of information.

The official definitions of InfoSec presented in Table 1 differ from the general definition (Section 2.1) and are inconsistent with each other. For example, the CNSSI definition includes in the scope of InfoSec protection of information systems, as well as information. An information system ac-

cording to the CNSSI is defined as *"a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information"*. Thus, *information resources* are in the scope of InfoSec according to the CNSSI definition, but this is explicitly captured neither in the general definition of InfoSec, nor in the definition suggested by the ISO/IEC.

Both, the CNSSI and ISO/IEC 27000 define InfoSec based on a set of security goals to be achieved. Thus, the essential discrepancy between the general comprehension of InfoSec and the definitions provided in the standards is that the general definition implies that information is secure if it is protected from all threats, whereas the standards imply that the information is secure if it complies with the certain security goals. This refers back to the fourth point stated in Section 2.1.

According to the definitions in Table 1, the scope of InfoSec defined by the ISO/IEC is wider than the scope defined by the CNSS. Apart from confidentiality, integrity and availability, the ISO/IEC also includes reliability, accountability, authenticity and non-repudiation in the realm of InfoSec, while the CNSS does not. For example, the breach of non-repudiation does not relate to any of the undesirable events stated in the CNSS definition. It is not mentioned in the CNSS definition of InfoSec as a security goal either.

Although the set of security goals associated with InfoSec in the CNSSI and ISO/IEC 27000 standard vary, they agree that the three fundamental goals of InfoSec are confidentiality, integrity and availability. ISACA clearly reflects this concept in its definition of InfoSec (Table 1). Consequently, the COBIT framework restricts the sphere of InfoSec to issues related to confidentiality, integrity and availability.

Since the standards correlate InfoSec with a certain set of security goals, then the origins of the goals and their interpretation becomes extremely important. The straightforward logical consequence of the steps to define an absolute list of security goals should be as follows: 1) identify all possible threats to information; 2) categorise the threats; 3) define a security goal for each category of threats. Due to the constant change in the environment, new threats constantly emerge and information received at the first step quickly becomes obsolete. Thus, security goals are only valid for the environment at a certain stage. This highlights the inadequacy of defining InfoSec purely through security goals, because any set of goals rapidly becomes incomplete in a transforming landscape and some threats stay out of the realm of InfoSec.

The definitions provided in the standards are used to define organisa-

tion's InfoSec program, strategy and policies. The limitation of InfoSec in this context leads to undesirable consequences that stem from overlooking essential threats and critical vulnerabilities that stay below the radar of InfoSec (Parker, 1998).

Defining the scope of InfoSec through certain security goals gives rise to two problems. First problem is the differing interpretations of the goals. The ISO/IEC 27000 standard and CNSSI definitions of *availability* and *confidentiality* correspond with each other, but the approaches to *integrity* in these two standards differ. The comparison of the definitions of integrity in Table 1 shows that the CNSS is concerned with the authenticity of data, while the ISO/IEC concentrates on the state of data, characterised by completeness and accuracy. Second problem: the CNSSI definition of InfoSec includes in its scope both information and information systems and, therefore, considering integrity in the definition of InfoSec, it is not clear whether it is integrity of information, or integrity of an information system, or both. If it is integrity of an information system, then to which part of the system it refers to: hardware, software, personnel or procedures.

In comparison to the general definition of InfoSec, the definitions suggested in the documents discussed narrow down the scope of the discipline because they define confidentiality, integrity and availability as the fundamental goals of InfoSec, rather than an overall protection of information. In the foreword to the first edition of Anderson's *Security Engineering* Schneier, wrote: *"You have to consider all the ways your system can fail. You have to look at everything backwards, upside down, and sideways*" (Anderson, 2001a, Foreword). It is obvious now that the ways a system can fail could not necessarily be characterised by a breach of confidentiality, integrity or availability. A definition of InfoSec, which is restricted to a certain set of security goals, prevents security specialists from having the necessary broad view of InfoSec. Therefore, the focus on the achievement of several pre-defined security goals, rather than on the achievement of adequate security is a flawed and dangerous approach, since it may lead to an oversight of some threats.

In Section 2.3, we discuss how academics and practitioners overcome the narrowing down of InfoSec to the CIA-triad. An overview of the comprehension of InfoSec in the academic and industry publications of the last twenty years is presented, and the recent trends in the evolution of InfoSec are distilled.

2.3. The Perception of Information Security in Academic and Industry Publications

Significant research was conducted over the last twenty years in order to establish the scope and to clarify the goals of InfoSec. Nevertheless, there is still no single commonly-agreed definition of InfoSec. The challenge of defining the scope and the goals of InfoSec stems, firstly, from the complexity of the discipline, secondly, from a variety of approaches to the discipline and, thirdly, from the evolving nature of the discipline.

Traditionally, InfoSec is defined via a set of security goals. Since the late 1970s, InfoSec has been rigorously associated with the CIA-triad (Whitman and Mattord, 2012). The major problem that arises from defining InfoSec via security goals is that the definition becomes obsolete as soon as new threats, not addressed by any of the existing security goals, evolve.

In recent years, there is a pronounced tendency to extend the scope of InfoSec beyond the CIA-triad since the latter is found to be no longer adequate (Parker, 1998; Whitman and Mattord, 2012) for a complex interconnected environment. A plethora of security goals is considered to be relevant to InfoSec and intensively discussed in the literature. Table 2 lists security goals associated with the discipline in the security-related publications. The publications are listed on the vertical axis in the chronological order. The horizontal axis lists security goals.

The analysis demonstrates the lack of an agreement about security goals and, consequently, about the scope of InfoSec. The variety of security goals discussed in the literature leaves the scope of InfoSec ambiguous. Moreover, the problem with varying definitions of the same security goals is also present in the academic publications, similar to the official documents, as discussed in Section 2.2.

The lack of clear InfoSec terminology gives rise to another problem: security goals are not clearly distinguished from security mechanisms. A clear distinction between a *security goal* and a *security mechanism* is required, as well as the association of a security mechanism with a certain security goal. This may enable the easier choice of an appropriate mechanism to pursue a certain security goal. This calls for a comprehensive model of InfoSec that helps to resolve these issues.

Going deeper into the discussion of security goals associated with InfoSec, it is important to highlight a substantial contribution to the clarification of InfoSec done by Parker (1998). Parker criticises the InfoSec definitions of

Table 2: Analysis of the literature in terms of goals associated with Information Security

Reference	Confidentiality	Integrity	Availability	Accountability	Assurance	Authentication	Non-repudiation	Authenticity	Reliability	Effectiveness	Efficiency	Compliance	Utility	Possession/Control	Authorisation	Awareness	Access	Identification	Accuracy	Administration	Information Classification	Anonymity	Audit	Safety	Other (not specified)
(Clark and Wilson, 1987)	X	X	X																						
(NCSC, 1991)	X	X	X																						
(McCumber, 1991)	X	X	X																						
(Parker, 1998)	X	X	X					X					X	X											
(Pipkin, 2000)	X		X	X											X	X	X	X	X	X					
(Schneier, 2000)		X				X															X	X	X		
(NIST, 2002)	X	X	X	X	X																				
(Gordon and Loeb, 2002)	X	X	X				X	X																	
(Avizienis et al., 2004)	X	X	X						X															X	
(ISO13335, 2004)	X	X	X	X			X	X	X																
(ITGI, 2007)	X	X	X						X	X	X	X													
(JF, 2007)	X	X	X	X		X									X						X				
(ISACA, 2008)	X	X	X																						
(ISO15408, 2009)	X	X	X																						
(ISO27000, 2009)	X	X	X	X			X	X	X																
(CC, 2009)	X	X	X																						X
(CNSS, 2010)	X	X	X			X	X																		
(Tiller, 2010)	X	X	X																						
(Dubois et al., 2010)	X	X	X	X			X																		
(HMG, 2011)	X	X	X																						
(Whitman and Mattord, 2012)	X	X	X					X					X	X					X						

being limited to the CIA-triad and claims them being dangerously incorrect. Parker introduces a new model of InfoSec that consists of six foundation elements: *confidentiality*, *integrity*, *availability*, *possession or control*, *authenticity* and *utility*. (Later, Kabay suggested the term *Parkerian Hexad* for the model, as a sign of respect to Parker.)

Possession or control is defined by Parker as *"the holding, control, and ability to use information"*. Consideration of possession as an additional security goals gains particular importance at the time of Cloud Computing. Utility is defined as *"usefulness of information for purpose"*. The definition of authenticity suggested by Parker, is much wider than the definitions of the same term provided in CNSS (2010) and ISO27000 (2009). A comparison of the definitions is presented in Table 3.

The definitions in the ISO/IEC 27000 standards and CNSSI correlate authenticity with the ability to verify the identity of the author. According

Table 3: Definitions of Authenticity

Standard/Term	Authenticity
ISO27000 (2009)	Property that an entity is what it claims to be.
CNSS (2010)	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
Parker (1998)	Validity, conformance, and genuineness of information.

to Parker, authenticity reflects *"the conformance to reality"* and *"extrinsic value or meaning of the information with respect to external sources"*. Parker states that even information provided by an authorised user, whose identity has been verified, may not necessarily comply with authenticity. That, for example, may happen in the case when an authorised user misrepresents information.

Parker (1998) argues that his model replaces the incomplete description of InfoSec limited to the CIA-triad. Albeit the model of InfoSec, suggested by Parker (1998), is not widely accepted, the research undertaken is fruitful because it addresses three issues, essential for the clarification of InfoSec:

1. The focus of the discipline is set on protection of information, rather than on protection of an information system. Parker consistently includes in his model properties of information and does not mix them with security mechanisms;
2. The importance of a complete and accurate definition of the discipline and, consequently, of the discipline's goals is highlighted and justified;
3. An attempt to extend the model of InfoSec and to address the limitations of the CIA-triad is undertaken. The overstepping the CIA-triad leads to the switch of InfoSec from the technical to the multidimensional discipline.

In agreement with Parker, Anderson (2001a) confirms that InfoSec is more than the CIA-triad. Anderson proclaims a multidimensional approach to InfoSec and sets forth that people, institutional and economic factors are no less important than the technical ones. Describing a security specialist, Anderson propones the requirement for such a specialist today to be familiar with business, management, and accountancy in addition to technology in

order to be able to communicate effectively with the top management as well as with the technical staff.

Anderson also is a pioneer of security economics. The economic perspective of security has been intensively discussed since the turn of the XXI century. Anderson (2001b) conducted an analysis of economic incentives behind some InfoSec failures and concluded that a purely technical approach to InfoSec is ineffective . Further, Anderson states that collaboration between managers, economists and lawyers is required in order to solve problems related to InfoSec. While Anderson (2001b) provides the general inside view on the economic incentives behind InfoSec, Gordon and Loeb (2002) look at the economics of investments into InfoSec. In 2002, they proposed the economic model that helps to determine the optimal amount of investment in InfoSec. In their work, Gordon and Loeb associate InfoSec with such goals as confidentiality, availability, authenticity, non-repudiation and integrity of information (Gordon and Loeb, 2002, p.439). The importance of economic motives is also recounted by Schneier (2008), who states that the number of vulnerabilities may only be reduced *"when the entities that have the capability to reduce those vulnerabilities have the economic incentive to do so"* . In addition to economics, Schneier reveals consideration of physiology and management to be essential for InfoSec (Schneier, 2000, 2008). Thus, in line with Anderson, Schneier confirms the multidimensional nature of InfoSec.

Schneier (2000) describes InfoSec as a process that includes: understanding of threats, design of polices and building of countermeasures to address the threats and, further, states that all the components of the process must fit together in order to achieve a best state of the overall process. He distinguishes the following goals of InfoSec: privacy, information classification (referred to as multilevel security), anonymity, authentication, integrity and audit (Schneier, 2000). Schneier lists among security goals not only properties of information (as it was consistently done by Parker (1998)), but also security mechanisms or abilities of information systems (e.g. authentication).

In line with Schneier, Pipkin (2000) defines InfoSec as a process, in this case as *"the process of protecting the intellectual property of an organisation"*. Pipkin includes in the scope of InfoSec and discusses in detail ten security goals: awareness, access, identification, authentication, authorisation, availability, accuracy, confidentiality, accountability and administration. This is another confirmation of a wide trend in InfoSec to combine security goals and security mechanisms as a result of considering information and information systems simultaneously to be subjects of protection in InfoSec.

Importantly, Pipkin (2000) takes InfoSec outside the hard perimeter of an organisation by defining that information should be protected *"in all its locations"*. In the present complex collaborative environment, information often intentionally leaves the safe boundaries of an organisation, but still requires protection. Pipkin (2000) also highlights a necessity of InfoSec flexibility in a constantly evolving environment.

Pipkin unveils InfoSec from the business standpoint and argues a need for InfoSec to become a business enabler and an integral part of a business. A similar approach to InfoSec is presented by Sherwood et al. (2005) who states that at present InfoSec, unfortunately, is often understood as a business preventer rather than a business enabler. According to Sherwood et al. (2005), InfoSec may help to raise trust of an organisation by customers and partners, and to allow an organisation to use effectively newly emerging technologies for a greater commercial success. InfoSec enables business by increasing its competitiveness. Delving deeper into the business approach to InfoSec, it should be understood that security of information is required not for its own sake, but for the advantages it gives to business (e.g. improved efficiency due to the exploitation of new technologies, increased trust from partners and customers). Sherwood et al. (2005) adopt a multidimensional and enterprise-wide approach to InfoSec and include in the scope of InfoSec, for example, such aspects of business as marketing and customer service. The authors declare protection of business assets and assistance with the achievement of business goals to be the main aim of InfoSec. Sherwood et al. (2005), in greater detail than Pipkin (2000), addresses the change of InfoSec approach related to the erosion of the hard perimeter of an organisation caused by active collaboration, operation in a distributed environment, and outsourcing of IT and other services. Pipkin (2000) and Sherwood et al. (2005), by the adoption of a business-oriented approach, support the tendency to extend the realm of the discipline. Thus, InfoSec is no longer considered purely from a technical perspective, but also from a managerial, system architect's and designer's points of view.

In line with others, Von Solm (2001) confirms the transition of InfoSec from purely technical to the multidimensional discipline and identifies thirteen closely interdependent dimensions of InfoSec:

1. The Strategic/Corporate Governance Dimension;
2. The Governance/Organisational Dimension;
3. The Policy Dimension;

4. The Best Practice Dimension;
5. The Ethical Dimension;
6. The Certification Dimension;
7. The Legal Dimension;
8. The Insurance Dimension;
9. The Personnel/Human Dimension;
10. The Awareness Dimension;
11. The Technical Dimension;
12. The Measurement/Metrics (Compliance monitoring/Real time IT audit) Dimension;
13. The Audit Dimension.

According to Von Solm (2001), the dynamic nature of InfoSec does not allow one to create a complete list of InfoSec dimensions at any given time. Despite the constant change of dimensions of the discipline the identification of different dimensions is desired because it will lead to the structuring of InfoSec complexity. Furthermore, only through addressing all InfoSec dimensions in a holistic manner could an organisation develop a secure environment.

The list of the InfoSec dimensions proposed by Von Solm (2001) may be extended with the following dimensions derived from the comparative analysis of (Anttila et al., 2004; Shoemaker et al., 2004):

1. The Physical Security Dimension;
2. The System Development Dimension which ensures that the security is built into the development process;
3. The Security Architecture Dimension;
4. The Business Continuity Dimension;
5. The Privacy Dimension.

Blakley et al. (2002) refers to InfoSec as a management of risks associated with information and claims that the ultimate task of InfoSec is the determination of the effectiveness of security mechanisms. This attitude to InfoSec was later captured in the term IA (see Section 3 for the detailed discussion.) Blakley et al. (2002) points out two reasons of the majority of security failures: (1) limited focus of the discipline (InfoSec generally concerned with technical and logical security mechanisms), and (2) ineffectiveness of security mechanisms. The first reason clearly testifies for a need in diversified solutions for security problems.

The shift of InfoSec from the technical to the broad, multidimensional discipline is also supported by Lacey (2009), who recounts that InfoSec "*draws on a range of different disciplines: computer science, communications, criminology, law, marketing, mathematics and more*". Lacey (2009) confirms the importance of technologies for protection of information, but emphasises even greater importance of the human factor which is based on the fact that all technologies are designed, implemented and operated by people. In addition to the human factor, Lacey also considers how organisational culture and politics affect InfoSec. Addressing the growing interconnectivity, Lacey (2009) gives an account of a recent Internet Age phenomenon - *de-perimeterisation*. De-perimeterisation refers to the erosion of the hard perimeter of an organisation in order to leverage achievement of business goals. Lacey (2009) points out an important switch in InfoSec from the protection of isolated enterprise systems to the protection of systems with open corporate boundaries.

De-perimeterisation is also intensively discussed by the Jerico Forum (JF) the international IT security association, that aims to develop solutions for secure business IT operations. According to the JF, de-perimeterisation is a result of *"a huge explosion in business collaboration and commerce on the Web"* (JF, 2011). The JF Commandments state that de-perimeterisation *"has happened, is happening, and is inevitable"* (JF, 2007) and provide a set of principles to be used for achievement of a *"good security"* in a collaborative, networked world. Although the JF follows a business-oriented approach, it still has a very technical standpoint and concentrates primarily on technical solutions of the issues related to de-perimeterisation (e.g. authentication and authorisation) (JF, 2007). Albeit de-perimeterisation is a recent phenomenon, a significant research already exists about the technical solutions that may be used for information protection in the de-perimeterised environment. Nevertheless, for the dimensions of InfoSec other than technical one, the effect of de-perimeterisation is not thoroughly investigated (Cherdantseva et al., 2011).

Thus, at the time of massive interconnection and collaborative information sharing, InfoSec becomes more challenging since information now needs protection not only within the safe organisation's perimeter, but also outside it. This important change within the InfoSec domain is outlined in (Pipkin, 2000; Sherwood et al., 2005; Lacey, 2009; JF, 2007, 2011; Cherdantseva et al., 2011).

The multidimensional nature and the broadening scope of InfoSec is also supported by Dlamini et al. (2009) who states that in the first decade of

the XXI century three areas became important for InfoSec: legal and regulatory compliance, risk management and information security management. As a consequence, the number of people involved in InfoSec is increasing. If previously there were only technical experts involved in InfoSec, at present managers, legal personnel, compliance regulators, human resources specialists are also involved in InfoSec.

In agreement with other authors, Tiller (2010) states the omnipresent nature of InfoSec and, most importantly, proclaims that in addition to a comprehensive approach InfoSec is required to be agile and adaptable to meet the requirements of continuously evolving business needs. The flexible adaptable nature of InfoSec, shown by many authors (Pipkin, 2000; Von Solm, 2001; Tiller, 2010), should be seen as a need to revise the approach to InfoSec as well its definition and its scope on the regular basis.

At the end of the XX and in the beginning of the XXI century a number of documents emerged escalating the importance of corporate governance: the Turnbull Guidance *"Internal Control: Guidance for Directors on the Combined Code"*, the American Institute of Certified Public Accountants (AICIPA) standards, the King report on Corporate Governance, the Organisation for Economic Co-operation and Development (OECD) Principles of Corporate Governance, the 8th audit directive of the European Union and the Sarbanes-Oxley Act. These documents attracted the attention of senior management to InfoSec problems that were previously deemed to be low level activities and the responsibility of technical personnel. The growing dependence of business on the IT systems led to the importance of InfoSec being recognised at the managerial level. This is depicted in many academic publications where InfoSec, among other dimensions, includes the governance, administration or management dimensions (Anderson, 2001a; Von Solm, 2001; Sherwood et al., 2005; Dlamini et al., 2009).

Analysis of the literature shows that there is a paradigm shift in InfoSec towards a coherent approach to information protection. Previously, the basic assumption was that the technology could provide *"absolute security"*. Nowadays, it is clear that the technology alone is insufficient for solving complex tasks of the discipline. Business needs, the human factor, economic incentives, cultural and organisational aspects should be taken into account in order to achieve an adequate protection of information. At present a comprehensive, multidimensional approach to the protection of information is required. At the end of this section, in order to summarise the review of the related literature and in order to portray the present state of InfoSec, we list

the recent discernible trends within the discipline:

1. InfoSec moves from a low-level technical activity and responsibility of computer specialists to a top priority activity dealt with at the strategic managerial level (Dlamini et al., 2009).
2. InfoSec becomes a multidimensional discipline. Aspects related to management (Pipkin, 2000; Sherwood et al., 2005; Tiller, 2010), marketing (Sherwood et al., 2005), economics (Anderson, 2001b; Schneier, 2008), physiology (Schneier, 2008; Lacey, 2009), law (Von Solm, 2001; Lacey, 2009), sociology (Theoharidou et al., 2005), criminology (Theoharidou et al., 2005; Lacey, 2009), mathematics (Anderson, 2001a; Lacey, 2009) and other disciplines are now in the scope of InfoSec.
3. InfoSec shifts from the protection of closed IT systems to the protection of open systems operating in a collaborative interconnected environment (Pipkin, 2000; Sherwood et al., 2005; ISACA, 2009).
4. As a result of the above, the CIA-triad is considered to be obsolete and not reflecting the complete scope of InfoSec (Parker, 1998; Anderson, 2001a). A plethora of security goals and security mechanisms is deemed to be relevant to InfoSec in addition to the CIA-triad (Table 2).

3. Information Assurance

Information Assurance (IA) is quite a new discipline, perhaps, the most striking feature of which is that everyone seems to have different opinion about what it actually is. In order to identify the scope and to understand the meaning of IA, in this section we follow the procedure similar to the one used to analyse InfoSec. First, the understanding of the term based on common English is examined. Then, we present the analysis of the definitions of IA provided by the official organisations, followed by the analysis of the comprehension of the discipline in the academic and industry publications. Finally, an adapted definition of IA is presented.

3.1. The Definition of Information Assurance based on Common English

For the purpose of working out the general definition of IA, we begin with the definition of the word assurance in the Oxford English Dictionary (2012):

- Assurance n.
  1. a positive declaration intended to give confidence; a promise;
  2. confidence or certainty in one's own abilities.

Confidence is defined as "*the feeling or belief that one can have faith in or rely on someone or something*" (Oxford English Dictionary, 2012). Based on the *"distilled knowledge and wisdom embodied in the dictionary definitions"* (Sherwood et al., 2005) we coin a general definition of IA:

Information Assurance is a discipline the main aim of which is to give confidence or certainty in information; to give belief that one can rely on data, knowledge, facts, and its meaning.

One important assumption that comes out of the above definition is that confidence in information must be based on confidence in all entities involved in the processes of information processing, storage and transmission. An entity, in this context, may mean a technical tool or system, a process, an individual or an organisation.

Similarly to the general definition of InfoSec, the definition of IA identifies a broad scope of the discipline. In this case, the general definition leaves a plethora of questions for discussion, for example:

- What are the properties that information should have in order for one to be able to rely on it?
- What actions should be undertaken on order to give confidence in information?
- What evidence is required to ensure confidence in information?

In order to find the answers for the above questions, in Section 3.2 we analyse the definitions of IA suggested in the official sources.

3.2. Information Assurance as defined in the official US and UK documents

The term IA was coined by the US Joint Staff in 1998 and for the first time appears in Joint Doctrine for Information Operations (Joint Pub, 1998). This document provided the classical definition of IA that for the first time declared five security goals, also known as the Five Pillars of IA: availability, integrity, authentication, confidentiality and non-repudiation.

In 2000, the term IA was included into the US National Information Systems Security Glossary, published by The National Security Telecommunications and Information Systems Security Committee (NSTISSC), which in 2001 was given a new name the Committee on National Security Systems (CNSS). Over the decade the definition has changed so that the latest definition refers to measures, rather than information operations as in the original

definition. Below is the definition of IA extracted from the CNSSI (CNSS, 2010):

Information Assurance - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

For the purposes of this definition, the following meanings also apply:

- Availability - The property of being accessible and useable upon demand by an authorized entity.
- Integrity - The property whereby an entity has not been modified in an unauthorized manner.
- Authentication - The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.
- Confidentiality - The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.
- Non-repudiation - Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

This original CNSS definition, based on the Five Pillars, remains the only rigorous definition of IA until present and, therefore, is highly cited. The analysis of the CNSS definition of IA is presented below. First, according to the CNSSI the scope of IA, in terms of security goals, is wider than the scope of InfoSec defined in the same document. In addition to the three security goals of InfoSec - confidentiality, integrity and availability - IA also aims to achieve authentication and non-repudiation. Second, the definition includes in the scope of IA not only information, but also explicitly states an information system as an object for control. The second sentence of the definition is particularly oriented on information systems and gives a technical sense to IA. Third, the Five Pillars of IA present an amalgamation

of security goals and security mechanisms. Whereas, *non-repudiation* is another security goal that aims to achieve a state where none of the entities may deny participation in the transaction, *authentication* is a security mechanism that helps to achieve such security goals as confidentiality, integrity and non-repudiation through the identity verification. The fact that security mechanisms are mixed in the definition with security goals is confusing. Adding to the confusion is the concentration on a certain security mechanism - authentication - and ignorance of other non-less important security mechanisms, e.g. authorisation and cryptography.

The CNSS definition of IA declares security goals, but does not define any methods to be used to achieve them. The clarification on that regard is found in (JS, 2000; DOD, 2002) which explain that IA may be achieved *"through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare."* The defense-in-depth concept was adopted by the US DoD from the Information Assurance Technical Framework (IATF) and is based on the long-existing military principle of multilayered protection of fortifications (Boyce and Jennings, 2002, p.39). As a result of the adoption of the defense-in-depth concept, IA includes into its realm such aspects as (JS, 2000):

- Risk management;
- Training, education and professionalism of the staff;
- Program, issue-specific and system-specific policies;
- Monitoring, management and administration;
- Assessment and audit.

In order to understand the concept of IA accepted by the UK government we examined *A National Information Assurance Strategy* that was published by the Cabinet Office in 2007 and the related documents. The glossary of *A National Information Assurance Strategy* (CSIA, 2007) defines IA as follows: *Information Assurance is the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users.*

According to this definition, IA has a very narrow scope and concerned only with the security of information systems. *HMG Security Policy Framework* (HMG, 2011), published by the Cabinet Office, also follows a similarly

narrow approach to IA, and concentrates on the risks associated with confidentiality, integrity and availability of information within an information system. IA here has a purely technical interpretation. A detailed analysis of *A National Information Assurance Strategy* shows that this document, in defining IA, puts a strong emphasis on the management of risks to information. That is derived from a definition of IA given in (CSIA, 2007, Foreword): *"Information Assurance is the term given to management of risk to information. Effective IA ensures that the opportunities provided by new technology can be exploited to maximum benefit.*" Further in the text CSIA (2007) inconsistently refers to the Five Pillars (rather than to the CIA-triad that is stated in the definition of IA provided in the glossary of the same document) and includes information in the scope of IA as well as information systems: *"The term 'information assurance' (IA) is used to describe confidence in the processes of information risk management. Effective IA should ensure appropriate levels of availability, integrity, confidentiality, non-repudiation and authentication of information and information systems."*

In fact, industry response to the IA strategy indicated that the key priorities of the strategy are not obvious and *"clouded by inconsistencies in delivery, belief or understanding."* (IACG, 2007)

In contrast with (CSIA, 2007; HMG, 2011), the *HMG Information Assurance Maturity Model and Assessment Framework* (HMG, 2010), proclaims a broader viewpoint on IA. It considers IA as a systematic, business enabling and dynamic approach to InfoSec which is not limited purely to information systems. According to (HMG, 2010), the IA scope is much wider than the scope defined in (CSIA, 2007) and comprise a diverse range of aspects including: leadership and governance; training, education and awareness; information risk management; through-life IA measures; assured information sharing; and compliance.

Albeit the uncertainty with the interpretation of IA in the UK official sources, it is clear that the perception of IA has a pronounced tendency towards technologies and information systems, and is focused on the management of risks to information, primarily associated with information systems. This is clearly declared in the vision of the *UK National IA strategy* for 2011 (CSIA, 2007): *"A UK environment where citizens, businesses and government use and enjoy the full benefits of information systems with confidence."*

Finally, according to the official sources, IA is concerned with a coherent multilayered protection of information. It is worth noting that the documents concentrate on protection of information in electronic form circulating within

computer systems and networks. The aspects such as risk assessment, monitoring and management are included in the scope of IA as a way of achieving a fair balance between security controls in the three layers of protection.

3.3. The Perception of Information Assurance in academic and industry publications

Since 1998, when the term IA was coined by the US military agencies, researchers and industry have been showing constant interest in IA. Although IA has existed for more than ten years, there is still no commonly agree understanding of it in the literature. In 2002, Kovacich stated: *"Information Assurance is one of the newly refined processes of information protection that has evolved from computer security and information system security. Is it InfoSec by another name, a subset, or just the other way around? There is some argument about that."* (Boyce and Jennings, 2002, Foreword). This argument is still valid today. In this section, delving deeper into the meaning of IA, we examine the perception of IA in academic and industry publications.

At the time when IA emerged, the environment was changing in two directions simultaneously: first, the world was getting more interconnected and, second, the importance of InfoSec was recognised at the managerial level (Section 2.3). Consequently, IA, which was deemed to address the change of the environment, received several interpretations, and, as a result, the focus and goals of the new discipline are noticeably inconsistent in various sources. Analysis of the related publications has identified three divergent interpretations of IA:

1. IA as a discipline dealing with the technical network-related security issues;
2. IA as a process of establishing confidence in information and information systems;
3. IA as a comprehensive management of InfoSec.

The third interpretation is the broadest one and is widely inclusive. It includes the technical aspect of IA, dominating in the first approach, and the establishment of confidence in information and information systems, dominating in the second approach. In some publications, an amalgamation of the approaches could be found. Nevertheless, in most cases the publication places a clear emphasis in its approach to IA which allows us to ascribed the work precisely to one of the three approaches. The approaches to IA listed above are outlined in detail in the following three sections.

3.3.1. Information Assurance as a discipline dealing with the technical network-related security issues

This interpretation is reflecting the change of the environment in terms of the growing interconnectivity and is solidly based on the original definition of IA, proposed by the US military agencies. IA here is considered as a subset of InfoSec, focusing on the network security. The Five Pillars (confidentiality, integrity, availability, authentication and non-repudiation) are the goals of the discipline. This approach was prevailing in the late 1990s and the early 2000s. It was and still is mainly supported by technical security specialists and government agencies.

The technical orientation implies that the discipline focuses on security of information systems and information within information systems. Consequently, security goals here describe the desirable properties of information systems, rather than properties of information. This, possibly, explains the fact that authentication, which is, in fact, a security mechanism, is included in the list of security goals.

In 2001, Maconachy et al. (2001) presented a model of IA. IA according to Maconachy is the next step of the InfoSec evolution. The model is an extension of the InfoSec model, originally proposed by McCumber (1991), where the CIA-triad is replaced with the Five Pillars. Maconachy et al. (2001) adopts a comprehensive and multidimensional approach to IA which stems from the defense-in-depth concept, but the goals of the discipline in this work are still limited to Five Pillars.

In 2002, McKnight (2002) defined IA from a purely technical viewpoint. Importantly, McKnight (2002) acknowledges that none individual viewpoint (including the technical one) would allow the creation of a correct picture of the discipline. Thus, the author recognises that IA extends beyond the technical domain. McKnight (2002) further states that in a broad sense IA incorporates the product, procedures, and policies that allow the timely transfer of information in an accurate and secure way among involved parties. McKnight (2002) claims that InfoSec is not the same discipline as IA, but does not discuss the distinctions between the disciplines. The author claims that technology and policies may change over time, whereas security goals will remain persistent. This claim is only partially true: although previously defined security goals (confidentiality, integrity, availability) stay consistent, the new security goals constantly evolve to reflect new threats. This issue is discussed in more detail in Section 2.

3.3.2. Information Assurance as a process of establishing confidence in information and information systems

This approach is based on a common understanding of the term *assurance* and correlates with the general definition of IA derived in Section 3.1. Here, IA is not an independent discipline, but an InfoSec subset which deals with (1) the classification of information by the level of confidence one may have in it or by correctness of information (Pipkin, 2000) and (2) the evaluation of the system's level of security (Anderson, 2001a).

In order to establish confidence in an information system, one needs to have an up-to-date model of evaluation criteria, as well as unambiguous security metrics and an agreed evaluation procedure. The Common Criteria for a long time has been serving as a model of evaluation criteria. This approach is clearly oriented on the evaluation and demonstration of the security level in order to gain trust of the internal and external parties (stakeholders, users, authorities, partners, customers etc.)

3.3.3. Information Assurance as a comprehensive management of Information Security

This interpretation reflects the recognition of the importance of InfoSec for business success and a need to address it at the managerial level. A certain element of *fashion* plays its role in the use of the term IA in this context. This approach to IA emerged in the early years of the XXI century and is widely adopted by the commercial world. The origins of this approach are rooted in the defense-in-depth concept. Here, IA is interpreted as comprehensive and systematic InfoSec management. The main aim of IA is not the achievement of pre-defined security goals, but the successful business operation and the overall protection of information (IAAC, 2002). This approach may be considered as an extension to the original concept of IA proposed by the DoD where IA is taken from the technical level, considering protection of information in the networked computerised systems, to the managerial level, concerned with the protection of business in the interconnected world.

This approach more than any other correlates with the general definition developed in Section 3.1, because only the comprehensive and systematic management of information and information systems may provide a sought-for confidence in information. In this approach technology is not the primary focus of the successful information protection. Here, InfoSec is deemed to be either a subset of IA or a concomitant discipline.

In 2002, the Information Assurance Advisory Council (IAAC), a UK-

based not-for-profit research organisation, in association with Microsoft published *"Benchmarking Information Assurance"* (IAAC, 2002). This document most prominently illustrates the discussed approach to IA. This document presents public and industry point of view on IA, and supports the argument about the little agreement on the concept and terminology related to IA. The IAAC states that the terms InfoSec and IT security over-emphasise the importance of confidentiality and miss out other problems such as accessibility or reliability, whereas IA overcomes these issues. Furthermore, the emphasis put on IT, also means that the risk to information is seen as a low-level activity, which is outside of the interests of senior management (IAAC, 2002). The survey conducted by the IAAC demonstrated that IA attracts more and more attention of top managers across multiple sectors, but more rapidly an integrated approach to information protection is accepted by smaller organisations.

Thus, the IAAC considers IA to be an activity dealt with at a higher level than InfoSec. InfoSec is a responsibility of computer specialists, whereas IA is a responsibility of senior management. IA is the systematic management of InfoSec, based on a holistic strategy. This also confirmed by the fact that BS7799 *Information security management. Code of practice for information security management systems* is considered to be the foundation of IA (IAAC, 2002). Interestingly, neither BS7799, nor the ISO/IEC 27000 series use the term IA or provide a definition of it. Nevertheless, other works (e.g. (IAAC, 2002)) refer to BS7799 and the ISO/IEC 27000 series as the IA standards, confirming the understanding of IA as a management of InfoSec.

Boyce and Jennings (2002) explain the concept of IA as it may be applied in the private and public sectors. The authors define IA as *"the process for protecting and defending information by ensuring its confidentiality, integrity, and availability. At its most fundamental level, IA involves protecting the rights of people and organisations."* Boyce and Jennings discern two main functions provided by IA: (1) the protection of an organisation's own rights (rights to survive, coexist and grow) and (2) the protection of other parties that interact with an organisation. The approach to IA presented in (Boyce and Jennings, 2002) spreads through both technical and managerial perspectives. The authors point out that at present, when technology is at the very core of any business, IA becomes an indispensable component of overall business performance. In terms of the goals of the discipline Boyce and Jennings, in addition to the CIA-triad also in detail discuss auditability (the ability to verify the activity of a security control), accountability (holding of individ-

uals liable for certain activities), access control, risk management, cost effectiveness, comprehensive and integrated approach, life-cycle managements, training and awareness, and continual reassessment. Although the authors still consider in detail the technical side of IA, they place the main emphasis on the importance of addressing information protection in the networked environment at the managerial level. Boyce and Jennings (2002) highlight that IA, by protecting information, a *"critical and strategic business resource"*, supports the mission of an organisation.

Tawileh and McIntosh (2007) also perceive IA as a separate discipline and the next step of the evolution of InfoSec, which in the process of its development and expansion, includes new aspects. The shift from InfoSec towards IA stems from "*the changes in the organisational environments and the information systems developed to serve these organisations*" (Tawileh and McIntosh, 2007) when in addition to the technological solutions, human and organisational aspects began to be taken into account.

Analysis of the literature shows that the commercial sector eagerly adopted the defense-in-depth concept which serves as the kernel of IA. The commercial world rather than to concentrate on the technical side of network protection and on the Five Pillars of IA, preferred to focus on the essence of IA - the comprehensive and systematic management of InfoSec based on the utilisation of a reasonable combination of the capabilities of people, operations and technology.

In 2011, a survey was conducted among one hundred of InfoSec and IA professionals. One of the aims of the survey was to identify the most commonly accepted perception of IA. The survey showed that the largest group of respondents (45 out of 100) is inclined to understand IA as a holistic, multidisciplinary and systematic approach to InfoSec. This approach corresponds with the interpretation of IA as a comprehensive management of InfoSec as outlined in this subsection. The full results of the survey are presented in (Cherdantseva and Hilton, 2013).

4. Information Security vs Information Assurance. The discussion.

In Sections 2 and 3, we have thoroughly studied the terms InfoSec and IA. In Section 5, the adapted definitions of InfoSec and IA have been presented. In this section, we conduct a comparison of the disciplines and attempt to describe the relationship between them. We also compare the disciplines with Computer Security (CS), a predecessor of InfoSec. The demonstration of the differences and similarities between the disciplines helps in the clarification of the scope and the specifics of each discipline. In this section, we endeavour to get beyond arguments about the definitions and into the understanding of the nature of InfoSec and IA.

Table 4 presents a comparison of CS, InfoSec and IA. In the horizontal axes, the table outlines the following characteristics for each discipline:

(1) **Dates**: specifies the approximate date since the discipline has existed;

(2) **Subject of protection**: describes what the discipline aims to protect;

(3) **Goals**: outlines the important goals of the discipline;

(4) **Type of information**: references the type of information to be protected;

(5) **Approach**: outlines the approach to information protection adopted within the discipline as well as the aspects of protection included in the approach;

(6) **Security Mechanisms**: describes security mechanisms that are exploited within the discipline in order to protect information;

(7) **Role within a business**: describes the role which the discipline plays within a business;

(8) **Responsible employees**: list the roles of employees, whose primary responsibility is protection of information. By the *dedicated staff* we refer to the employees who deals with information protection as their primary duty (e.g. Chief Information Security Officer (CISO) and employees under his/her management);

(9) **Involved employees**: lists employees who are involved in information protection;

(10) **Drivers**: describes the drivers behind security decisions;

(11) **Flow of security decisions**: describes how security decisions are taken within an organisation.

As described in Section 3, IA has three distinct interpretations. For the purpose of the comparison in this section, we adopt the perception of

Table 4: Comparison of Computer Security, Information Security and Information Assurance

Discipline Characteristics	**Computer Security**	**Information Security**	**Information Assurance**
Dates (approx.)	Since the early 1960s	Since the 1980s	Since 1998
Subject of protection	Computers	Information and information systems	Business as a whole
Goals	Reliability	Confidentiality, Integrity, Availability (Authenticity, Accountability, Non-repudiation, Reliability)	Overall business protection
Type of information	Electronic	Primarily electronic	All types
Approach	Strictly technical	Domination of the technical approach, initial attempts to consider soft aspects (e.g. human factor, administration)	All-encompassing multi-disciplinary systematic approach
Security Mechanisms	Technical	Primary focus is on technical security mechanisms; initial consideration of organisational and human-oriented mechanisms	All available (technical, organisational, human-oriented, legal)
Role within a business	Supporting system	Supporting system, often inducing some restrictions on business	An integral aspect of business, business enabler
Responsible employees	Technical staff	Dedicated staff and technical staff (often in addition to the other duties)	Senior management and dedicated staff
Involved employees	Technical staff	Senior management, dedicated and technical staff	All employees with an organisation
Drivers	Technical-needs driven	Security-needs driven	Business-needs driven
Flow of security decisions	Bottom-Top (senior management is not concerned with technical aspects of security)	Bottom - Top (security measures are initiated by technical specialists, based on their experience and passed to senior management for approval)	Top - Bottom (security measures are initiated by senior management based on risk analysis and implemented by relevant departments)

IA as a comprehensive and systematic management of InfoSec. There is no such thing as "absolute security", but there is adequate security which is sufficient to address an organisation's risk appetite within the existing technical, cultural, legal and organisational constraints. IA aims to identify

the level of adequate security and the best ways to achieve it, whereas InfoSec deals with the achievement itself.

In parallel with the formation of IA, InfoSec has been changing and growing in terms of the scope and goals. As a result, many characteristics that are outlined in Table 4 for IA are often attributed to InfoSec as well. This makes the border between InfoSec and IA very vague. It is hard to conduct a comparison of these disciplines due to their natural changeability. Nevertheless, in this section we attempt to do the comparison by fixing the understanding of InfoSec according to the official definitions discussed in Section 2.2. CS is included in the comparison in order to demonstrate the evolution of attitude to information protection over the longer period and to draw the prominent change in this attitude.

Table 4 shows that whereas CS is concerned with the protection of computers, InfoSec is concerned with the protection of information and information systems. IA, in its turn, deals with the protection of a business as a whole. Consequently, the goals of the disciplines are differing. CS aims to achieve reliability of hardware and software. The main goals of InfoSec are confidentiality, integrity and availability of information, along them a wide range of goals is attributed to InfoSec including authenticity, accountability, non-repudiation etc. IA addresses protection of all aspects of the business. If the sphere of responsibilities of InfoSec specialists is confined to protection from expected threats, e.g. unauthorised access (confidentiality), unauthorised modification (integrity) and unauthorised denial-of-use (availability), IA specialists are accountable for the organisation's resistance not only to known, but also to unknown and unexpected threats. Thus, the cornerstone principle of the contemporary approach to information protection may be summarised in the phrase *"Expect the Unexpected!"* (Neumann, 1995).

"Information exists both inside and outside the computer and has to be protected wherever it travels" (Pipkin, 2000, p.13). Hence, information protection should not be restricted to considering information within computer systems only. Whereas CS and InfoSec concentrate on the protection of electronic information, from the IA perspective information of any type (electronic, paper, knowledge etc.) requires adequate protection.

The approach to information protection adopted within InfoSec is primarily focused on technical solutions to security issues. The protection of information systems and networks is certainly important, but represents only one facet of the problem. In order to achieve adequate security the full spectrum of issues related to information protection should be addressed. In response

to this call, IA adopts an all-encompassing, multidisciplinary and systematic approach to information protection. As a result, the security mechanisms exploited by the disciplines vary from solely technical mechanisms within CS to all available security mechanisms within IA.

CS, as well as InfoSec, plays the role of a supporting system within a business. InfoSec is also often deemed to be a business preventer (Sherwood et al., 2005). The transformation of InfoSec from a business preventer into a business enabler and an integral part of a business is clearly depicted within the IA concept. For IA, security is not a self-contained goal; security contributes to the achievement of business objectives and security measures address the real business risks (Parker, 1998, p.30). Moreover, IA looks for a subtle compromise between productivity and security.

In terms of responsibility for information protection, IA promotes the organisation-wide culture of InfoSec. Thus, all employees and not only the dedicated staff should recognise the importance of InfoSec and their personal responsibility for information protection. Senior management and such departments as IT, legal, marketing, human resources, compliance, accounting, risk management, quality control, business continuity, physical security and privacy are often engaged in the implementation of some parts InfoSec strategy and policies without explicitly acknowledging that. IA integrates InfoSec-related activities under an overarching administration. The interrelationships between the activities of the various departments are approached in a structured manner which helps to improve the InfoSec posture of an organisation and to reduce security costs by the elimination of duplicated activities.

The flow of security decisions within CS is described as bottom-top since technical security decisions are generally out of the scope of the senior management and are deemed to be a low-level activity. InfoSec has changed the situation slightly, the senior management began to be involved in security decisions, but still the decisions are mostly originated at the bottom, by technical staff, and passed to the senior management for financial approval. IA promotes the opposite flow of security decisions: security decisions are taken by the senior management based on a thorough risk assessment and business needs analysis and then passed to the relevant departments for implementation. Thus, security decisions within the IA concept are business-needs-driven, whereas InfoSec solutions are often based on the security needs and ignore or even contradict business needs.

Finally, the importance of the comparison and understanding of the dif-

ferences between the disciplines is explained. The widely-known saying declares that the right diagnosis is a half of the treatment. Therefore, at an initial stage it is important to describe carefully the problem of information protection, as well as to identify available means that could be exploited for the solution. The evolution of the approaches to information protection, presented via a comparison of CS, InfoSec and IA helps one to familiarise with the state-of-the-art in information protection. An appreciation of the differences between InfoSec and IA assists in the judgement about whether the organisation's approach to information protection is up-to-date with the latest trends. It also helps to clarify the sphere of responsibility and interests of InfoSec and IA practitioners and researchers.

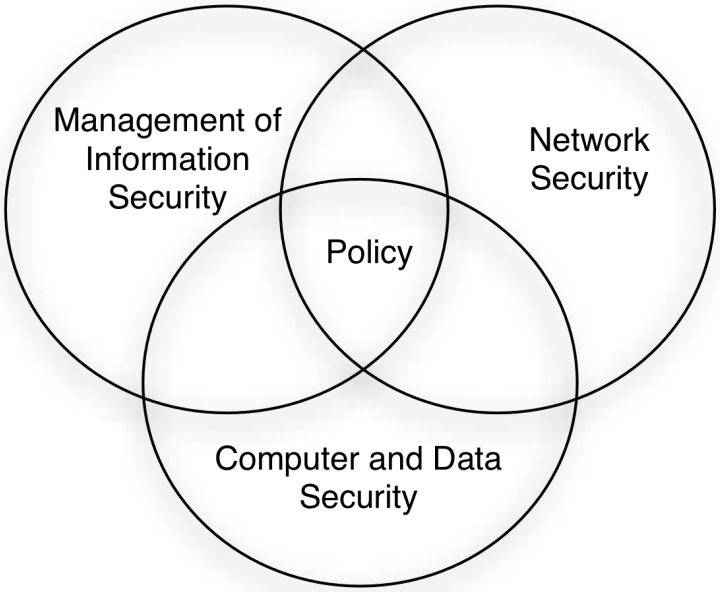
The usage of the term IA to refer to a comprehensive and systematic management of InfoSec is debatable. The term InfoSec may be used under the assumption that it reflects the broad scope including management as well. Nevertheless, the use of the term IA in the context described is more desirable, since it demonstrates, without additional explanations, that there are differences between the approaches to information protection. The distinction between InfoSec and IA comes down to the distinction between the actions taken to protect information and the management of those actions. First, this notion brings the understanding of the need to the management in general, and second, it outlines the variety of security mechanisms and actions that could be used for information protection. IA helps to overstep the limitation to the technical perception of InfoSec problems and takes them to the higher managerial level. The use of the right term will lead to a better understanding of the underlying problem and to the optimal choice of the preventive measures.

The principal question of the interrelation between InfoSec and IA is quite difficult. For example, (Whitman and Mattord, 2012) see InfoSec management (IA as we refer to it) to be one of the components of InfoSec along with computer & data security and network security (Figure 1).

The survey of InfoSec and IA professionals (introduced in Section 3.3) invited participants to describe the relationship between InfoSec and IA. The analysis of the responses indicates that there is no single widely accepted understanding of how these two disciplines relate to each other (Cherdantseva and Hilton, 2013).

The problem of the mutual relationship between InfoSec and IA is debatable and deserves discussion. On the one hand, contrary to the most popular perception of the relationship between the disciplines, as identified

Figure 1: Components of Information Security (Whitman and Mattord, 2012, p.9)

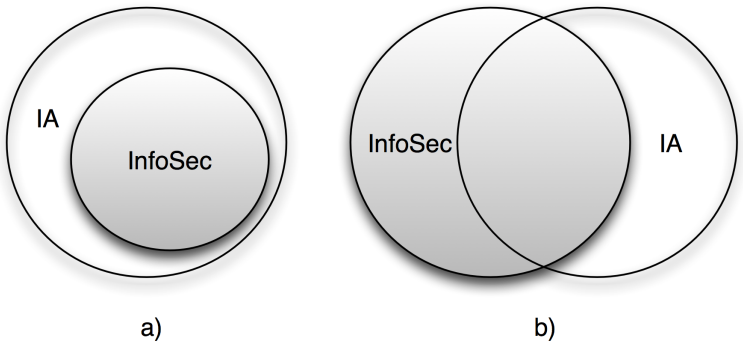


in the survey (Cherdantseva and Hilton, 2013), it is our opinion that IA is a discipline of a wider scope which includes InfoSec (Figure 2a). The fact that the management of actions designed to address information protection would include the actions themselves and that both activities have a common goal supports this approach. Thus, IA may be seen as an umbrella term.

On the other hand, InfoSec and IA may be deemed to be different disciplines that have a significant overlap in their interests (Figure 2b). The argument to support the second approach is that both disciplines consider certain issues that are out of the scope of another discipline. For example, (1) the technical details of the firewall technology are out of the scope of IA, while in the scope of InfoSec and (2) the calculation of the optimal investments in security is out of the scope of InfoSec, while in the sphere of the IA interests. The authors of the paper are more inclined to the second approach, although the second approach gives rise to another question about how the joint area of InfoSec and IA should be referred to.

In 2001, a group of representatives of fifteen U.S. undergraduate Information Technology programs, IEEE, ACM and ABET began work to formalise Information Technology as an accredited academic discipline (Dark et al.,

Figure 2: The Relationship between Information Security (InfoSec) and Information Assurance (IA)



2005). One of the challenges was to define the area of knowledge referred to as *security*. Since the term *security* was deemed too restrictive and not reflecting the broad range of concepts included in the discipline, the group turned its attention to the term Information Assurance, which was at that time used by U.S. NSA and CNSS. In 2005, it was decided to label the area of knowledge, covering security in IT education programs, as *Information Assurance and Security* (Dark et al., 2005). A model of Information Assurance developed by Maconachy et al. (2001) was accepted as the model of the Information Assurance and Security knowledge area. If we adopt the perception of IA as the management of InfoSec and InfoSec as referring to technical and practical aspects of information protection, then the use of the term *Information Assurance and Security* to cover the joint area of both disciplines (Figure 2b) is sensible.

The authors are not aware of other sources that attempt to clarify the interrelationship between InfoSec and IA and draw a border between them. This section presents only the authors' opinion on the subject. It does not pretend to be the absolute truth and is open to discussion. The main aim of this discussion is to attract the attention of InfoSec and IA experts to the important question of the scope of InfoSec and IA, their interrelationship and the border between the disciplines.

5. The Adapted Definitions of Information Security and Information Assurance.

Albeit that, at the first glance, the meaning of InfoSec is fairly intuitive, the scope and the goals of the discipline are ambiguous. The analysis undertaken shows that the lack of an agreed definition and an unclear scope of InfoSec are the problems troubling the discipline. Until now, nobody seems to have produced a single, all-encompassing definition of InfoSec, possibly due to the complexity and persistent alteration of the discipline. The definitions provided in the standards are not adequate and do not reflect the broad scope of the discipline described by the academic and professionals (Section 2.2). We have not found a clear rigorous definition of InfoSec in either the academic or industry publications (Section 2.3). Some of the definitions of InfoSec found in academic publications are listed in Table 5.

The examination of the term IA, based on the analysis of the standards, academic and industry publications, confirmed that IA has various interpretations. IA was originated in the US military agencies as a discipline dealing with the technical security issues in the new networked environment. Later, the defense-in-depth concept, which lies at the very heart of IA, was taken up by the commercial world and intensively supplemented with the new findings. At the turn of the century, the commercial sector recognised a need for a comprehensive and systematic approach to managing InfoSec. IA, which was coined at the same time, was deemed to be a modern response to that growing need. As a result, IA transformed from a discipline dealing with the exploitation of people, operations and technology capabilities in order to protect information in the networks to the discipline of a comprehensive and systematic management of InfoSec needed in order to improve overall business security and productivity. Thus, over the last decade IA evolved from the technical discipline dealing with the network security issues into the broad discipline which now includes soft aspects like administration, training and education.

Further, research has showed that, at present, there is no definition of IA which reflects the discipline in its broadest sense. The original definition of IA, based on Five Pillars, does not reflect the complexity and scope of the discipline in full. Similarly with the definitions of InfoSec, the definition based on a certain set of security goals has become obsolete very rapidly in the current changing environment. Moreover, the definition based on the Five Pillars limits not only the goals of the discipline, but also security

Table 5: The Existing Definitions of Information Security

Source	**Definition of Information Security**
Pipkin (2000)	Information Security is the process of protecting the intellectual property of an organisation.
Blakley et al. (2002)	...information security is a risk management discipline, whose job is to manage the cost of information risk to the business.
Anderson J. (2003)	A well-informed sense of assurance that information risks and controls are in balance.
Venter and Eloff (2003)	Information security is the protection of information and minimises the risk of exposing information to unauthorised parties.
Shoemaker et al. (2004)	Rather than being a separate study, information security draws from a number of other academic domains. These include: computer science, computer architecture, forensics, cryptography, knowledge and information theory, business, mathematics, military science, law and ethics, software engineering, statistics and all things having to do with the Internet.
Sherwood et al. (2005)	Information security is the enabling technology of electronic business [p.5]. Information systems security is only a small part of information security, which in turn is but one part of a wider topic: business assurance[p.24].
Dlamini et al. (2009)	Information security has evolved from addressing minor and harmless security breaches to managing those with a huge impact on organisations' economic growth. ... Does this mean information security is a new field or just another "fad"? No, information security is neither new nor a "fad". What is new is its broader focus and wider appeal.
Chahino and Marchant (2010)	Information Security is a discipline governing the framework for the continuous cycle of safeguarding information and ensuring related regulatory compliance.
Kazemi et al. (2012)	Information security is not just a technical issue, but a very important management issue, its main purpose is to create a secure information environment.
Whitman and Mattord (2012)	Information Security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology. [p.8]

mechanisms that may be used. The evolving nature of the discipline and its broad scope should be captured in the definition. Ideally, the relationship between InfoSec and IA should be clarified.

In order to summarise the enhanced understanding of the burgeoning ar-

eas of InfoSec and IA, and to address the drawbacks of the existing definition, we endavour to develop the adapted contemporary definitions of the disciplines. The definitions, by no means, attempt to introduce new knowledge or concepts. They only attempt to synthesise and express in a concise form the outcomes of a thorough analysis of the security-related literature presented in the previous sections. Below we present a two-part adapted definition of InfoSec and an adapted definition of IA:

Information Security *is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats.*

Threats to information and information systems may be categorised and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability.

Information Assurance *is a multidisciplinary area of study and professional activity which aims to protect business by reducing risks associated with information and information systems by means of a comprehensive and systematic management of security countermeasures, which is driven by risk analysis and cost-effectiveness.*

We conclude this section by reviewing the advantages of the elaborated definitions. The advantages of the proposed two-part definition of InfoSec:

- The definitions explicitly reflects the multidisciplinary nature and the diverse scope of InfoSec in its current reincarnation (1) by declaring a wide range of security mechanism that could be exploited for information protection and (2) by outlining an extensive list of security goals. The set of security goals is adopted from the detailed examination of the evolution of security goals presented in a companion paper *The Evolution of Information Security Goals from the 1960s to Today* (Cherdantseva and Hilton, 2012).

- The definition puts the correct emphasis among the priorities of InfoSec

by stating the protection of information from threats as a primary goal of InfoSec and protection of information systems as a consequent goal.

- The definition clearly distinguishes security goals from security mechanisms which may be exploited in order to achieve security goals.

- The definition distinguishes four types of security mechanisms:

    1. *Technical* (e.g. biometrics, firewalls, PKI, digital signature, malicious code, virus and intrusions detection systems etc.)
    2. *Organisational* (e.g. strategy, policies, processes, audit, physical security, recovery plans etc.)
    3. *Human-oriented* (e.g. training, education, motivation, ethics, culture etc.)
    4. *Legal* (e.g. legislation, Job contracts, non-disclosure agreements, service-level agreements,)

    The lists of security mechanisms within each type is by no means exhaustive and only intended to give an idea of a variety of security mechanisms available.

- Following the traditional approach to defining InfoSec, the proposed definition refers to security goals. (Anderson J., 2003) states that the definition of InfoSec should provide more guidance about the objectives of InfoSec programs. In addition to naming security goals, the second part of the definition explains the origins of security goals. This information is essential for understanding, particularly, for newcomers to the field, but omitted in all known to us definitions of InfoSec.

- Although the definition outlines the currently relevant set of security goals, it does not limit the scope of InfoSec to the listed goals. The refined definition leaves the space for the natural changeability of the discipline and for open-mindedness among security experts by declaring a need of a regular revision of security goals.

- The definition reflects the growing trend in InfoSec towards the open, de-perimeterised environment by pointing out the need to protect information outside an organisation's perimeter as well as inside it.

The advantages of the proposed definition of IA:

- Importantly, the definition of IA declares the protection of a business as the ultimate goal. Although the security goals of InfoSec are inherited by IA, since IA has a wider scope and incorporates InfoSec (see Section 4 for the explanation), it is important to outline in the definition of IA that the reason behind all IA activities is the overall protection of business.

- The definition declares a need in a comprehensive and systematic management of security countermeasures. *Comprehensive* management means that security mechanisms of all available types should be exploited, the scope should not be limited to technical mechanisms. *Systematic* management refers to the fact that information protection should be addressed consistently at every stage of the system life-cycle.

- The definition declares two main drivers behind security decisions:

  Risk analysis - IA does not attempt to eliminate all risks, the risks should be prioritised, according to the organisation's specifics, and reduced to an acceptable level;

  Cost-effectiveness - IA does not attempt to achieve security at any price, but in a most efficient and cost-effective way.

- The suggested definition clarifies the relationship between InfoSec and IA. If InfoSec is concerned with the development and implementation of security mechanisms, IA is concerned with the design of a sensible and effective combination of security mechanisms. In short words, it is possible to say that IA is a comprehensive and systematic management of InfoSec. Thus, the adapted definition fully supports the approach to IA exposed in Section 3.3.3.

6. Conclusion

The problem with defining terms may seem to be far from the real world and has no practical value. We would argue with that. Looking in depth, the paper tries to tackle a vital problem - that a restricted vision or misunderstanding of such important domains as InfoSec and IA will lead to different perceptions and behaviours that will introduce vulnerabilities into our world of interconnected systems. How could an organisation trust, for example, security strategy and policy creation or implementation to an employee who

does not recognise the complexity of the security domain. In support of our argument, Anderson J. (2003) in the paper "Why we need a new definition of information security" declares that the absence of a clear definition of InfoSec which identifies what InfoSec professionals are in charge of and on what organisations spend significant funds is causing confusion and problems. Furthermore, according to (Anderson J., 2003), the lack of a generally accepted definition of InfoSec is one of the reasons for difficulties with measurement of InfoSec outcomes.

Although both disciplines - InfoSec and IA - have existed for some time the interrelationship between them is not obvious and not easy to trace in the literature. The numerous informal discussions on the Internet, that aim to find the meaning of InfoSec and IA, the differences between them and the goals of the disciplines, confirm that the answers to these questions are important for individuals interested in information protection, but are not straightforward. Although experts in the field, who benefit from years of learning and experience, may see no need in the discussion like this, for the newcomers this discussion provides a valuable insight into InfoSec and IA.

As stated in the introduction, the aim of this work is to clarify the existing misinterpretations of the terms InfoSec and IA and to present a clear, contemporary picture of both disciplines, by identifying the scope and goals, and by formulating an adapted definition of each discipline. In order to answer the research question, a thorough analysis of InfoSec and IA, based on common English, was conducted. We analysed US, UK and European InfoSec and IA related official publications and standards, and discussed the perception of the disciplines in the related academic and industry works, published over the last twenty years.

The analysis has shown that the existing definitions of InfoSec and IA do not fully reflect the complex subject of the disciplines and, therefore, dangerously restrict the scope of the disciplines. The analysis has also allowed us to achieve the main research goal - to elaborate the contemporary adapted definitions of InfoSec and IA (Section 5). This paper contributes to the fields of InfoSec and IA by providing an analysis of the related literature and by giving an account of the state-of-the-art in both disciplines. This research ventures beyond previous works by distinguishing and describing three approaches to IA.

We hold firmly to the belief that the business and academic domains may benefit from the overview of the latest trends in InfoSec and IA, and from the definitions of the disciplines presented in the paper. The paper may

further the understanding of security professionals and young academics in the disciplines. The research, generally, promotes the culture of InfoSec and IA by increasing awareness about the disciplines. Furthermore, the adoption of an integral and consistent viewpoint of information protection described in the paper may increase the ability of business to foresee and, consequently, to avoid many threats to information in a continuously changing environment.

Business requires a growing number of highly educated InfoSec and IA specialists with knowledge of new technologies and negotiation skills (PwC, 2010). The need for training in a diverse range of subjects (e.g. information risk management, forensics, end-user awareness etc.) also increases. Therefore, InfoSec and IA higher education programs, in order to meet the expectations of prospective students and employers, should be kept up-to-date with the recent trends of the disciplines. The perception of InfoSec and IA should be agreed between business and academia in order to assist graduates to comply with industry requirements. The discussion presented in this paper contributes to the more precise interpretation of InfoSec and IA and clarifies the scope, goals and approach of each discipline. We hope that this paper will catalyse a fruitful discussion and development of the InfoSec and IA education programs, which cover the entire body of knowledge associated with the disciplines and not only some parts of it. Having an agreed area for research, teaching and practice raises the status of the disciplines and enhances their further development.

Security is always context-specific, therefore some may argue that the definition of InfoSec will always be organisation specific and is a matter of a lexicon. This argument may be valid only in a "closed" environment, when an information system of an organisation is completely isolated from the rest of the world. For a collaborative de-perimeterised environment, where organisations share information, integrate information systems and business processes, a harmonised understanding of InfoSec expressed in a mutually-agreed definition is essential.

For example, Company A believes that the scope of InfoSec is limited to the CIA-triad, Company B, who exchange sensitive information with Company A, expects that authenticity, non-repudiation and accountability are also covered by security policies. Customers of both companies expect that their privacy is protected. This sort of dissimilar expectation about InfoSec exists. We do not claim that an agreed definition on its own would solve all the problems, but it is good to start a discussion and is a solid stepping stone on the way towards a synchronised approach to information protection.

In order to summarise the outcomes of the study, we draw attention to two important conclusions. First, this research highlights the importance of clear and precise definitions of such crucial disciplines as InfoSec and IA. Incomplete definitions may lead to a perilous circumscription of the discipline (Section 2.3). As alluded to in the previous sections, the definitions of InfoSec and IA tend to set a list of security goals in order to define a realm of the fields. The reason is obvious: security specialists must be provided with a rigorous framework of responsibilities. The drawback of this approach is that some threats and vulnerabilities, in particular newly emerging ones, may be overlooked and omitted because they stray out of the boundary of InfoSec and IA.

This leads us to the second essential conclusion: since InfoSec and IA are inherently open and evolving arenas, any definition, although providing a scrupulous framework and stating security goals, has to promote open-mindedness among experts dealing with InfoSec. The ultimate aim of both disciplines is to protect the life-blood of an organisation its strategic information - by the exploitation of all available security mechanisms.

As a direction for further research, we see a call for an up-to-date conceptual model of InfoSec and IA, which will depict the complexity and multidimensional nature of the disciplines in an increasingly interconnected environment. A model allowing the structuring of the existing body of knowledge of the disciplines discussed here will be a significant contribution to the art and science of information protection.

References

Anderson, J.M. Why we need a new definition of information security. Computers & Security, 22 (4), pp. 308-313. 2003

Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley Publishing, 2001.

Anderson R. Why Information Security is Hard ? An Economic Perspective. Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual, pp. 358-365.

Anttila, J., Kajava, J. and Varonen, R.. Balanced Integration of Information Security into Business Management. Proceedings of the 30th EUROMICRO Conference, pp.558 - 564, 2004.

Avizienis A., Laprie J.-C. , B. Randell B., and Landwehr C. E.. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable Sec. Comput., vol. 1, no. 1, pp. 11-33, 2004.

Boyce J. and Jennings D.: Information Assurance: Managing Organizational IT Security Risks. Butterworth-Heinemann (Elsevier Science), 2002.

Blakley B., McDermott E. and Geer D. Information Security is Information Risk Management. In Proceedings of the 2001 workshop on New Security Paradigms NSPW '01. pp. 97 - 104. ACM, NY, USA 2001 doi:10.1145/508171.508187

Common Criteria (CC) for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1. Revision 3. July 2009.

Chahino, M. and Marchant, J. CIS conference presentation, Washington DC. 2010.

Cherdantseva Y. and Hilton J., The Survey of Information Security and Information Assurance Professionals, 2011.

Cherdantseva Y. and Hilton J., The Evolution of Information Security Goals from the 1960s to today. Unpublished. February, 2012.

Cherdantseva Y., Rana O., Hilton J.. Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success. ISSE Securing Electronic Business Processes, Prague 22-23 November 2011. Highlights of the ISSE 2011 Conference, pp. 201-213.

Cherdantseva Y. and Hilton J., The Survey of Information Security and Information Assurance Professionals, 2011. In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing. (2013)

Clark D. and Wilson D.. A Comparison of Commercial and Military Computer Security Policies. Proc. IEEE Symposium on Security and Privacy, 1987, pp.184-195.

Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

Collins English Dictionary Online, http://www.collinsdictionary.com.

CSIA. A National Information Assurance Strategy. Crown, 2007.

Dark M., Ekstrom J. and Lunt B.. Integration of Information Assurance and Security into the IT2005 Model Curriculum. SIGITE '05 Proceedings of the 6th conference on Information technology education. ACM New York, NY, USA, 2005.

Dlamini M.T., Eloff J.H.P., Eloff M.M. Information security: The moving target. Computers and Security, vol. 28, iss. 3-4, May-June 2009, pp. 189-198.

U.S. Department of Defense (DOD). Directive Number 8500.01E October 24, 2002. Certified Current as of April 23, 2007.

Dubois, E., Heymans, P., Mayer, N., Matuleviius, R.. A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Intentional Perspectives on Information Systems Engineering. pp. 289-306. Springer, 2010.

FRC. The Turnbull guidance as an evaluation framework for the purposes of Section 404(a) of the Sarbanes-Oxley Act. Available online at http://www.frc.org.uk/documents/pagemanager/frc/draft_guide.pdf [accessed on 15. 03.2012].

Gartner, Inc. Forecast Overview: Security Infrastructure, Worldwide, 2010-2016, 2Q12 Update.

Gordon L. and Loeb M..The Economics of Information Security Investment. ACM Transactions on Information and System Security, vol. 5, No. 4, November 2002, pp. 438-457.

The Cabinet Office. HMG Information Assurance Maturity Model and Assessment Framework. Crown Copyright. Version 4.0, 27 May 2010.

The Cabinet Office. HMG Security Policy Framework. v.5.0, Crown Copyright. February, 2011.

Information Assurance Advisory Council (IAAC) in association with Microsoft. Benchmarking Information Assurance. 2002.

Information Assurance Collaboration Group (IACG). Industry Response To The HMG Information Assurance Strategy and Delivery Plan. A report by the IACG Working Group On The Role Of Industry In Delivering The National IA Strategy (IWI009). 2007.

ISACA. Glossary of Terms, 2008. Available online at http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf [accessed on 10.07.2011].

ISACA. An Introduction to the Business Model for Information Security, 2009.

$(ISC)^2$. The 2011 $(ISC)^2$ Global Information Security Workforce Study. 2011.

ISO/IEC 13335-1:2004. Information technology - Security techniques - Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management.

ISO/IEC 15408-1:2009. Information technology-Security techniques-Evaluation criteria for IT security. Part 1: Introduction and general model.

ISO/IEC 27000:2009 (E) Information technology - Security techniques - Information security management systems - Overview and vocabulary.

IT Governance Institute (ITGI). COBIT 4.1. Excerpt. 2007.

Jericho Forum (JF). Jericho Forum Commandments. 2007. Available online at https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf [accessed 5 April 2012].

Jerico Forum (JF). The What and Why of De-perimeterization. Available online at http://www.opengroup.org/jericho/deperim.htm [accessed on 16.04.2011].

Joint Pub 3-13. Joint Doctrine for Information Operations. USA, 1998.

The U.S. Joint Staff (JS). Information Assurance through Defense in Depth. Feb 2000.

Kazemi M., Khajouei H. and Nasrabadi H.. Evaluation of information security management system success factors: Case study of Municipal organization. African Journal of Business Management. 6(14), pp. 4982-4989, 2012. Available online at http://www.academicjournals.org/AJBM. Accessed on 20.11.2012.

Lacey D.. Managing the Human factor in information security. J. Wiley and Sons Ltd. 2009.

Maconachy W., Schou C., Ragsdale D. and Welch D.. A Model for Information Assurance: An Integrated Approach. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, U.S. Military Academy, West Point, NY, 5-6 June, 2001.

McCumber J., Information Systems Security: A Comprehensive Model. Proceeding of the 14th National Computer Security Conference, NIST, Baltimore, MD, October, 1991.

McKnight, W.. What is information assurance? CrossTalk, The Journal of Defense Software Engineering, pp.4-6. 2002.

National Computer Security Center (NCSC). Integrity in Automated Information Systems. C Technical Report 79-91 Library No. S-237,254(IDA PAPER P-2316). September, 1991.

Neumann P.. Computer-Related Risks. ACM Press/Addison Wesley. 1995.

NIST. Risk Management Guide for Information Technology Systems. Special Publication 800-30. July 2002.

Oxford Dictionaries Online, http://oxforddictionaries.com.

Parker D.. Fighting Computer Crime. New York, NY, John Wiley and Sons, 1998.

PwC. Information Security Breaches Survey 2010. Technical report. 2010

Pipkin D.. Information Security: Protecting the global enterprise. Hewlett-Packard Company, 2000.

SANS Institute. An Overview of Sarbanes-Oxley for the Information Security Professional. 2004. Available online at http://www.cs.jhu.edu/ rubin/courses/sp06/Reading/soxForInfoSec.pdf [accessed on 15.03.2012].

Schneier B.. Secrets and Lies. John Wiley and Sons, 2000.

Schneier B.. Schneier on Security. Wiley Publishing. 2008.

Shaw, A. Data breach: From notification to prevention using PCI dss. Columbia Journal of Law and Social Problems, vol.43, iss. 4, June 2010, pp. 517-562.

Sherwood J., Clark A., Lynas D.: Enterprise Security Architecture: A Business-Driven Approach. CMP Books, 2005.

Shoemaker, D., Bawol, J., Drommi, A., et al., A Delivery Model for an Information Security Curriculum. In Proceedings of the Third Security Conference, (Las Vegas, Nevada, USA), Information Institute, 2004.

Sony Computer Entertainment America. Letter to the Subcommittee on Commerce, Manufacturing and Trade of the U.S. House of Representatives. May 3, 2011. Available online at: http://www.flickr.com/photos/playstationblog/sets/72157626521862165 [accessed on 15.03.2012].

Tawileh A. and McIntosh S.. Understanding Information Assurance: A Soft Systems Approach. Proceedings of the United Kingdom Systems Society 11th International Conference, September 3-5, 2007, Oxford University, UK.

Theoharidou M., Kokolakis S., Karyda M. and Kiountouzis E.. The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 2005. 24, pp. 472-484.

Tiller J. S.. Adaptive Security Management Architecture. Auerbach Publications. 2010

Trustwave Holdings, Inc. The Trustwave 2012 Global Security Report. 2012.

Venter H.S. and Eloff J.H.P. A taxonomy for information security technologies. Computers & Security, 22 (4). pp.299-307. 2003.

Von Solms B.. Information Security - a multidimentional discipline. Computers & Security, vol: 20, iss.: 6, pp: 504-508. Elsevier, 2001.

Whitman M.E. and Mattord H. J. , Principles of Information Security, 4th edition, Course Technology, Cengage Learning, 2012.