From information security to cyber security

Article *in* Computers & Security · October 2013

DOI: 10.1016/j.cose.2013.04.004

2 authors, including:

Johan van Niekerk
Nelson Mandela University
54 PUBLICATIONS **297** CITATIONS

COMPUTERS & SECURITY XXX (2013) 1–6

Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

From information security to cyber security

*Rossouw von Solms**, *Johan van Niekerk*

School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth 6031, South Africa

ARTICLE INFO

Article history:
Received 26 November 2012
Received in revised form
10 April 2013
Accepted 11 April 2013

Keywords:
Information security
Cyber security
Cybersecurity
Cyber-Security
Computer security
Risk
Threat
Vulnerability

ABSTRACT

The term *cyber security* is often used interchangeably with the term *information security*. This paper argues that, although there is a substantial overlap between cyber security and information security, these two concepts are not totally analogous. Moreover, the paper posits that cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself. In information security, reference to the human factor usually relates to the role(s) of humans in the security process. In cyber security this factor has an additional dimension, namely, the humans as potential targets of cyber attacks or even unknowingly participating in a cyber attack. This additional dimension has ethical implications for society as a whole, since the protection of certain vulnerable groups, for example children, could be seen as a societal responsibility.

1. Introduction

Cyber security has become a matter of global interest and importance. Already more than 50 nations have officially published some form of strategy document outlining their official stance on *cyberspace*, *cyber crime*, and/or *cyber security* (Klimburg, 2012). The Whitehouse (2011) has outlined a cyber strategy that provides the stance of the United States of America (USA) on cyber-related issues and outlines a unified approach to the USA's engagement with other countries on cyber issues. The United Kingdom (UK) lists cyber security as a top priority and has committed £650 million over four years for a transformative National Cyber Security Programme (Minister for the Cabinet Office and Paymaster General, 2011). However, very few of these sources seem to make a distinction between the concepts of *cyber security* and *information security* or the relationship between them.

In most literature, cyber security is used as an all-inclusive term. Definitions of this term vary, for example the *Merriam Webster dictionary* defines it as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack". The International Telecommunications Union (ITU) defines cyber security as follows:

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and

* *Corresponding author*. Tel.: +27 41 504 3604; fax: +27 41 504 9604.
E-mail addresses: Rossouw.VonSolms@nmmu.ac.za, Rossouw@nmmu.ac.za (R. von Solms), johan.VanNiekerk@nmmu.ac.za (J. van Niekerk).

0167-4048/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.04.004

maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality ITU, 2008.

These definitions are very similar to that of *information security*. This paper will explore the definition of information security in depth and then argue that the boundaries of cyber security as a concept are wider than those of information security in terms of how it is formally defined. This viewpoint is supported by the international standard ISO/IEC 27032:2012(E).

This paper will specifically focus on the underlying nature of security in general and will attempt to show, by means of examples, that the assets cyber security aims to protect include an additional dimension which extends beyond the formal boundaries of information security. Further, this paper asserts that both humans in their personal capacity and society at large can be directly harmed or affected by cyber security attacks, whereas this is not necessarily the case with information security where harm is always indirect. The authors view such a disambiguation as an important contribution to the common body of knowledge for the field of information and cyber security. Such a body of knowledge provides a "basis for understanding terms and concepts" in the subject area and thus acts as a "taxonomy of topics relevant to professionals around the world" (Theoharidou and Gritzalis, 2007).

2. Information security

The aim of information security is to ensure business continuity and minimise business damage by limiting the impact of security incidents (Von Solms, 1998). Information security can be defined in a number of ways, as highlighted below.

2.1. *Information security defined*

The international standard, ISO/IEC 27002 (2005), defines information security as the preservation of the confidentiality, integrity and availability of information (ISO/IEC 27002, 2005, p. 1). In the context of ISO/IEC 27002 (2005), information can take on many forms. It can be printed or written on paper, stored electronically, transmitted by post or electronic means, shown on films, conveyed in conversation, and so forth (ISO/IEC 27002, 2005, p. 1).

Whitman and Mattord (2009) define information security as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" (Whitman and Mattord, 2009, p. 8). These authors (2009) also identify several critical characteristics of information that give it value in organisations. These characteristics include the confidentiality, integrity and availability of information, as mentioned in the definition provided in ISO/IEC 27002 (2005), but are not limited to these three characteristics only. According to Whitman and Mattord (2009, p. 8), ensuring the confidentiality, integrity and availability of information, also known in information security as the CIA triangle, has traditionally been the industry standard. "The security of these three characteristics of information is as important today as it has always been, but the CIA triangle model no longer adequately addresses the constantly changing environment of the computer industry" (Whitman and Mattord, 2009, p. 8). Accordingly, Whitman and Mattord (2009) add accuracy, authenticity, utility and possession to the list of information characteristics that needs to be protected.

A few concepts in the above definitions need closer examination. Firstly, it should be clear that information security is not a product or a technology, but a process (Mitnick and Simon, 2002, p. 4). According to Wood (2004) information security used to be a strictly technical issue. However, as the use of computers and networks evolved, the process of securing these computers and networks also had to evolve to extend beyond only the technical. The process of information security may require the use of certain products, but is not something that can be bought off the shelf.

The second important factor to note about the above definitions is that information security is commonly defined in terms of the properties or characteristics that secure information should have. These usually include the confidentiality, integrity and availability of information, but can include additional characteristics.

It is important to note that there is a difference between information security and information technology (or information and communication technology) security.

2.2. *Information and communication technology security defined*

Information and communication technology (ICT) security deals with the protection of the actual technology-based systems on which information is commonly stored and/or transmitted. The international standard ISO/IEC 13335-1 (2004) defines ICT security as all aspects relating to defining, achieving and maintaining the confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of information resources (ISO/IEC 13335-1, 2004, p. 3). Since information security includes the protection of the underlying information resources, it can be argued that ICT security is a sub-component of information security.

The definition of ICT security is thus very similar to that of information security. However, additional characteristics, which in this context could be better described as services that should be provided by secure information resources, are added to the definition. These include non-repudiation, accountability, authenticity and reliability. Dhillon (2007, p. 19) also refers to the concept of data security as denoting the protection of the actual data in an information system. Since the definition given in Dhillon (2007, p. 19) includes most of the characteristics in the definition for information technology security, and because the security of underlying data is to

Please cite this article in press as: von Solms R, van Niekerk J, From information security to cyber security, Computers & Security (2013), http://dx.doi.org/10.1016/j.cose.2013.04.004

a large extent reliant on the overall security of the information system on which the data resides, it can be argued that the term *data security* is in fact used in Dhillon (2007) to refer to the same concept as that which ISO/IEC TR 13335-1 (2004) calls ICT security.

From the definitions discussed in Sections 2.1 and 2.2 it should be clear that there is a difference between securing information resources and securing ICT resources. A secure information resource could include any entity from which information is received or to which information is sent. A secure information technology resource is a secure information resource that *happens to reside on an information technology system*. It is also important to note that, in terms of ICT-based systems, the information alone cannot be deemed to be secure unless all resources and processes dealing with that information are secure as well.

As mentioned earlier, the first three characteristics, confidentiality, integrity and availability, are commonly known as the CIA triangle model, which has been considered the industry standard for computer security since the development of the mainframe (Whitman and Mattord, 2009, p. 8). The additional characteristics have been added to the definition to address organisations' additional security needs in today's inter-networked business environment. A clear understanding of the meaning of all the above-mentioned characteristics (and/or services) is essential to an understanding of information and ICT security, as without the confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information resources, information cannot be deemed secure. All of the above (including the accuracy, utility and possession of information) play an integral role in information security and should be deemed equally important. It is, however, possible for one or more of these characteristics or services to be more applicable in specific scenarios than others, depending on the nature of the information itself. For example, the integrity of inflationary statistics is of obvious importance for economists, whilst the confidentiality of the same data appears to be unimportant because everyone would probably be allowed to have access to such information. However, by definition, a breach of confidentiality only occurs if an unauthorised entity obtains the information. Since everyone would be an authorised user of inflationary statistics, in this case, the confidentiality of the information would actually be maintained. In an organisational context, ensuring the security of the organisation's information is thus not a case of deciding which characteristics or services are applicable, but rather of defining the authorised entities, as well as other parameters for any given piece of information, correctly.

When analysing ICT security, as described above, it is clear that various threats are targeting related vulnerabilities and, eventually, have a negative impact on ICT infrastructure. In this case it is clear that the technological infrastructure is deemed to be the asset that needs protection. Accordingly, in ICT security the ICT is the asset that is secured. Fig. 1 depicts this relationship.

In the case of information security, ICT is the infrastructure that processes, stores and communicates information. In this case it is information that is deemed to be the asset that requires protection, as depicted in Fig. 2. Information and

Fig. 1 – Information and communication technology security.

communication technology can in this case be classified as, among other things, a vulnerability that is targeted by various threats in an attempt to compromise the asset, that is, information.

Thus, it is important to note that, in the case of information security, information is the asset that is to be secured.

The following sections will argue that, in cyber security, the nature of the threats, vulnerabilities and assets differs from that of information security.

3. Cyber security

As mentioned earlier, many current publications dealing with cyber security use the term *cyber security* interchangeably with the term *information security*. If cyber security is synonymous with information security it would be reasonable to assume that cyber security incidents could also be described in terms of the characteristics used to define information security. Thus, a cyber security incident would, for example, also lead to a breach in the confidentiality, integrity or availability of information.

This is true for the majority of cyber security related threats a user and/or organisation might be exposed to. However, it is the contention of this paper that there are cyber security threats that do not form part of the formally defined scope of information security. This section will briefly present a few scenarios as examples:

3.1. *Scenario 1 – cyber bullying*

Cyber bullying has become a major concern to modern society (Martin and Rice, 2011). According to Martin and Rice (2011), several recent studies have found that technology is increasingly used to bully, "cause embarrassment, invoke harassment and violence, and inflict psychological harm". This could lead to "severe and negative impacts on those victimized".

The need to address cyber bullying has become widely acknowledged as a cyber security problem and is even mentioned specifically in the UK Cyber Security Strategy (Minister for the Cabinet Office and Paymaster General, 2011, p. 26). However, being bullied in cyberspace does not constitute a loss of confidentiality, integrity or availability of information. Instead, the target of such activities is the user him/herself. Accordingly, cyber bullying results in **direct** harm to the **person** being bullied.

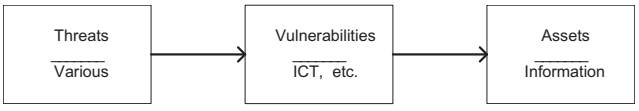

Fig. 2 – Information security.

Please cite this article in press as: von Solms R, van Niekerk J, From information security to cyber security, Computers & Security (2013), http://dx.doi.org/10.1016/j.cose.2013.04.004

3.2. Scenario 2 – home automation

Advances in ICT, as well as advances in the field of electronics, have given rise to a multitude of home automation applications (Jiménez et al., 2011). Many of these allow home owners to integrate home security systems, hot water geysers, fridges, stoves, televisions and other appliances with web-based management systems. Unfortunately, the increased convenience of managing one's home via the web is accompanied by the increased risk that someone might gain unauthorised access to such systems and cause harm. This harm could range from "pranks" like turning off the hot water, to serious crimes like turning off the security system in order to burgle the home.

Once again, in this case one can argue that the victim's information is not necessarily negatively affected. Instead, **other assets** of the victim are the target of the cybercrime.

3.3. Scenario 3 – digital media

One of the industries that have been directly affected by the improved sharing of information is the entertainment industry. Every year enormous amounts of potential revenue are lost to the sharing of illegal movies, music and other forms of digital media. This illegal sharing does not necessarily affect the confidentiality, integrity or availability of the shared media; however, it does directly affect the financial wellbeing of the legal owner of the rights to the specific media. Self-justification of illegal activities, like copying media illegally, could even act as a catalyst that makes it easier to perform other illegal acts in future (Ariely, 2012).

In this case it could be argued that the victim of the cybercrime is more than just the party whose intellectual property is being compromised. It even extends to an attack on the value system (both ownerships rights and the underpinning ethics of the perpetrators) that is being negatively affected.

3.4. Scenario 4 – cyber terrorism

In the USA critical infrastructure is defined as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof" (Department of Homeland Security, 2011). Infrastructure that delivers electricity and water, controls air traffic, or supports financial transactions is seen as "critical life sustaining infrastructures" and all directly depend on underlying communications and network infrastructure (The Whitehouse, 2011, p. 3). The protection of such critical infrastructure forms an important part of cyber security and is included as an important national imperative in national cyber security strategies (Minister for the Cabinet Office and Paymaster General, 2011, p. 39; The Whitehouse, 2011, p. 13).

Cyber terrorists or enemy specialists may target a country's critical infrastructure via cyberspace. This could either be indirectly, for example by influencing the availability of information services using denial-of-service attacks or, more directly, through an attack on the national electricity grid. In the case of attacks against such critical infrastructure, the loss entails not only of that of the integrity or availability of information resources, but also that of access to such critical services. In this case, it is neither the information itself nor the individual information user that is at risk, but rather the wellbeing of society as a whole. A good example of such attacks is the attacks on Estonia in April/May of 2007.

These scenarios deal with a specific aspect of cyber security where the interests of a **person, society or nation, including their non-information based assets,** need to be protected from risks stemming from interaction with cyberspace. This serves to highlight the difference between information security and cyber security.

4. From information security to cyber security

All security is about the protection of **assets** from the various **threats** posed by certain inherent **vulnerabilities**. Security processes usually deal with the selection and implementation of security **controls** (also called countermeasures) which help to reduce the **risk** posed by these vulnerabilities (ISO/IEC 27002, 2005; Farn et al., 2004; Gerber and Von Solms, 2005).

In the case of ICT security, the asset(s) that need to be protected are the underlying information technology infrastructure (see Fig. 1). Information security, on the other hand, extends this definition of the assets to be protected to include all aspects of the information itself. It thus includes the protection of the underlying ICT assets, and then goes **beyond just the technology** to include information that is not stored or communicated directly using ICT (see Fig. 2).

However, as demonstrated in the scenarios above, in cyber security the assets that need to be protected can range from the person him/herself to common household appliances, to the interests of society at large, including critical national infrastructure. In fact, such assets include absolutely anyone or anything that can be reached via cyberspace.

It is thus the assertion of this paper that the term *cyber security* is related, but **not** analogous, to the term *information security*. In cyber security, information and ICT are the underlying cause of the **vulnerability**. It is still possible for the assets dealt with in security to include information itself, or even information and communication infrastructure. However, the single most defining characteristic of cyber security is the fact that all assets that should be protected need to be protected because of the vulnerabilities that exist as a result of the use of the ICT that forms the basis of cyberspace.

These vulnerabilities can even affect intangible assets. For example, cyber security adds an important ethical dimension, because problems such as cyber bullying extend beyond the law and present an ethical issue that society, in general, needs to deal with. This ethical dimension extends to problems like botnets. Being part of a botnet does not always mean that the confidentiality, integrity, availability or other characteristics of one's information resources have been directly affected; it is quite possible that a botnet may only "steal" clock cycles on a computer while it would otherwise be inactive. However, if such a botnet is used to commit a crime, the owner of the computer in question might be an unknowing accomplice.

Please cite this article in press as: von Solms R, van Niekerk J, From information security to cyber security, Computers & Security (2013), http://dx.doi.org/10.1016/j.cose.2013.04.004

Nonetheless, this ethical dimension of cyber security is not the only intangible asset which needs to be protected. For example, a review of 19 different national cyber security strategy documents has shown that the protection of the **trust** that citizens have in using cyberspace for commercial purposes is seen as vital by all the nations whose policies were covered by this review (Klimburg, 2012).

Taking the above-mentioned discussion and scenarios into account, it is clear that in cyber security the asset that needs to be protected extends beyond the boundaries of the information per se as defined for information security. Firstly, from the first and second scenarios it should be clear that, in cyber security, assets include the personal or physical aspects, both tangible and intangible, of a human being. In addition to this, as can be seen in the third and fourth scenarios, cyber security also includes the protection of societal values (intangible) and national infrastructure (tangible). In cyber security the assets thus include both tangible and intangible assets relating to the wellbeing of either the individual or society at large. In the case of cyber security, the information itself can be classified as a vulnerability. In all the above scenarios, the compromising of information leads directly to an impact on the asset, in this case possibly a human in his/her personal capacity, or society in general, as depicted in Fig. 3.

Just as information security expanded on the concepts of ICT security in order to protect the information itself, irrespective of its current form and/or location, cyber security needs to be seen as an expansion of information security. Cyber security should be about protecting more than just the information, or information systems resources, of a person/organisation. Cyber security is also about the protection of the person(s) using resources in a cyber environment and about the protection of any other assets, including those belonging to society in general, that have been exposed to risk as a result of vulnerabilities **stemming from the use of ICT**. The relationship between these three overlapping concepts is illustrated in Fig. 4.

It is clear from the discussion above that in information and communication security the asset to be secured is the underlying technology. In the case of information security, the asset(s) to be secured is the information together with the underlying technologies. However, in the case of cyber security, the goal is clearly not to secure cyberspace but rather to secure those that function in cyberspace, whether individuals, organisations or nations.

As the role of ICT becomes increasingly ubiquitous in society, the roles that humans play in the underlying information and ICT-related security processes will continually expand. In ICT security, the role of humans has been largely restricted to that of a threat. In information security this role has grown to become an increasingly integral part of the supporting systems and thus humans have become a vulnerability. Today, in cyber security, humans and human

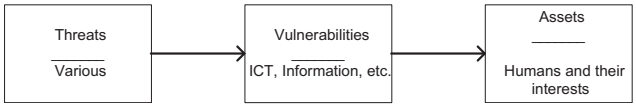

Fig. 3 – Cyber security.

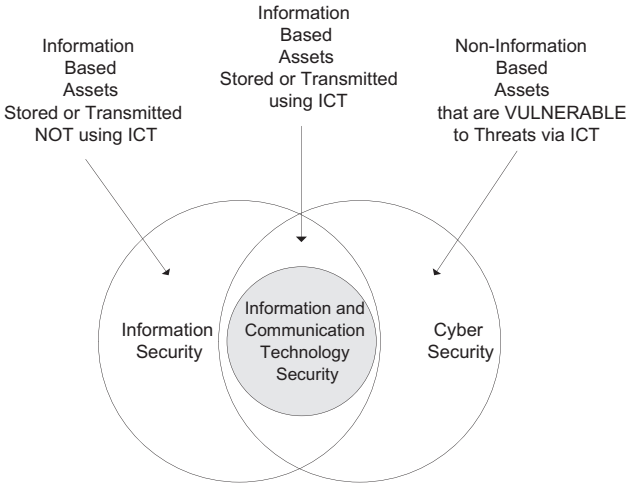

Fig. 4 – The relationship between information and communication security, information security, and cyber security.

societies have grown to become part of the assets that need to be protected. Although humans are still deemed to be both a threat and a vulnerability, nowadays they are also deemed to be an asset that needs to be protected in cyberspace.

In light of the above, cyber security can be defined as the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace.

From the definition above it is clear that cyber security is far more extensive than any of the information and/or ICT security that it encompasses. The human element, including national interests, is playing an ever-increasing role in cyber security and certainly the current set of international standards and best practices is not comprehensive enough to secure cyberspace.

5. Conclusion

This paper explored the definitions of both information security and ICT security. The paper then argued that cyber security, despite often being used as an analogous term for information security, differs from information security. Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities. Cyber security, on the other hand, is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace.

REFERENCES

Ariely D. The (honest) truth about dishonesty: how we lie to everyone – especially ourselves. HarperCollins; 2012.

Please cite this article in press as: von Solms R, van Niekerk J, From information security to cyber security, Computers & Security (2013), http://dx.doi.org/10.1016/j.cose.2013.04.004

Department of Homeland Security. Critical infrastructure. Washington, DC: Department of Homeland Security. Cited 23 November 2012. Retrieved from: http://www.dhs.gov/files/programs/gc_1189168948944.shtm; 2011.
Dhillon G. Principles of information systems security. John Wiley & Sons; 2007.
Farn K-J, Lin S-K, Fung AR-W. A study on information security management system evaluation: assets, threat and vulnerability. Computer Standards & Interfaces 2004;26(6):501–13. http://dx.doi.org/10.1016/j.csi.2004.03.012.
Gerber M, Von Solms R. Management of risk in the information age. Computers & Security 2005;24(1):16–30. http://dx.doi.org/10.1016/j.cose.2004.11.002.
ISO/IEC. ISO/IEC TR 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, JTC 1, SC27, WG 1 2004.
ISO/IEC. ISO/IEC 27002: code of practice for information security management 2005.
ISO/IEC. ISO/IEC 27032:2012(E) information technology – security techniques – guidelines for cybersecurity. Geneva, Switzerland: ISO/IEC; 2012.
International Telecommunications Union (ITU). ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity 2008.
Jiménez M, Sánchez P, Rosique F, Álvarez B, Iborra A. A tool for facilitating the teaching of smart home applications. Computing Applications in Engineering Education 2011. http://dx.doi.org/10.1002/cae.20521.
Klimburg A, editor. National cyber security framework manual. NATO CCD COE Publications; 2012. December.
Martin N, Rice J. Cybercrime: understanding and addressing the concerns of stakeholders. Computers & Security 2011;30:803–14.
Minister for the Cabinet Office and Paymaster General. The UK cyber security strategy: protecting and promoting the UK in a digital world. Cited 12 February 2012. Retrieved from: http://www.cabinetoffice.gov.uk/sites/default/files/resources/WMS_The_UK_Cyber_Security_Strategy.pdf; 2011.
Mitnick K, Simon W. The art of deception: controlling the human element of security. Wiley Publishing; 2002.
The Whitehouse. International strategy for cyberspace: prosperity, security, and openness in a networked world. Cited 12 February 2012. Retrieved from: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; 2011.
Theoharidou M, Gritzalis D. Common body of knowledge for information security. Security & privacy. IEEE. Retrieved from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4140992; 2007.
Von Solms R. Information security management (3): the code of practice for information security management (BS 7799). Information Management & Computer Security 1998;6(5):224–5.
Whitman ME, Mattord HJ. Principles of information security. 3rd ed. Thompson Course Technology; 2009.
Wood CC. Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Computer Fraud & Security 2004;2004(1):16–7.

Rossouw von Solms is the Director of the Institute for ICT Advancement at the NMMU. Rossouw has published and presented in excess of one hundred and fifty academic papers in journals and conferences, both internationally and nationally. Most of these papers were published and presented in the field of Information Security.

Johan van Niekerk is a member of faculty in the Department of Information Technology at the Nelson Mandela Metropolitan University. He holds a PhD in Information Technology. His research focus is the human factors in information security and he has been publishing regarding this topic for the past decade. He actively participates in many cyber security awareness campaigns and is a member of several professional bodies and associations involved in this field.

Please cite this article in press as: von Solms R, van Niekerk J, From information security to cyber security, Computers & Security (2013), http://dx.doi.org/10.1016/j.cose.2013.04.004