IDENTIFYING CRITICAL DATA AND DATABASES – A PROPOSAL FOR A RISK-BASED THEORY OF IMPLEMENTING CHAPTER IX OF THE ECT ACT

Mzukisi Niven Njotini
LLB LLM
Doctoral Candidate
Lecturer, Department of Jurisprudence
University of South Africa (UNISA)

SUMMARY

South Africa adopts meaningful measures to prevent and/or alleviate attacks to its critical data and databases. The measures are embodied in Chapter IX of the Electronic Communications and Transactions Act 25 of 2001.[1] The Chapter IX measures encumber the Minister of Communications to perform innumerable functions, *inter alia*, to identify and classify critical data and databases. However, this article submits that the Chapter IX measures are founded and places (unlimited) reliance on a stagnant or inflexible approach. Such an approach assumes that a process to identify and classify critical data and databases is a product of guesswork. Put differently, the Chapter IX measures uses a common-knowledge or one-size-fits-all approach as an aid to identify and classify critical data and databases. By so doing, Chapter IX of the ECT Act fails to recognize that a holistic and flexible approach or framework is indispensable in a process to identify and classify critical data and databases.

1 INTRODUCTION

The rise of Information and Communication Technologies (ICTs) results or has resulted in the aggregating of vast amounts of information[2] or data[3] into centralized and/or connected databases. Centralized and connected databases offer financial benefits as well as convenience of accessibility and wide availability of ICT protocols or hyperlinks. Increasingly, the databases

[1] Hereinafter "the ECT Act".

[2] For an interesting definition of the term "information", see in general Sieber "The Emergence of Information Law – Object and Characteristics of a New Legal Order" in Lederman and Shapira (eds) *Law, Information and Information Technology* (2001) 10–11.

[3] The notion "data" means the electronic representation of information in any form (s 1 of the Electronic Communications and Transactions Act 25 of 2002 (hereinafter "the ECT Act")). The notion "any form" is, however, not defined in the ECT Act. For purposes of this article the concept "any form" will therefore mean automated or non-automated form.

have become critical and essential to the operation of many organizations or businesses. The interlinking and interdependency of these databases mean that the databases may become critical. This criticality can either relate to the functioning of the organization concerned or to other organizations, and individuals relying on the database. The former may include citizens who may wish to use the facilities of that organization. The extensive accessibility of these databases and their critical nature makes them susceptible to attack from criminal intruders. These intruders adopt and implement a combination of both passive and active attacks to critical databases (cyber-attacks or attacks).[4] Passive intrusions, on the one hand, are demonstrated by or take place in cases where an information system or network is infiltrated surreptitiously and without detection.[5] On the other hand, active intrusions occur by, *inter alia*, altering or adapting an information system or network.[6] The effect of both these cyber-attacks generally is to perturb or alter the appropriate functioning of critical databases. These attacks then have unfavourable effects to the organization or related individual. For example, a collapse or an attack to data and/or databases does not only affect the organisation but moreover becomes widespread and potentially poses or generates serious consequences to a society.[7]

It is not necessary to prevent a database from functioning in order to cause substantial harm. An alteration or interruption of databases will be sufficient to cause unpleasant effects on the organization, including any other organization that relies on that database. Such alteration or interruption must, however, be of such nature that a country's national safety and security or the security of its citizens is hindered.[8] Furthermore, this national or citizen's safety and security must be of such importance that the security of critical data and databases is sustained. Put differently, the national or citizen's safety and security must warrant that steps be taken to ensure that the data is protected and that databases are managed properly. Therefore, the steps or measures to secure databases must mitigate the impact of database mismanagement and cyber-attacks, for example computer hacking,[9] pharming or spoofing,[10] phishing[11] and cyber-terrorism.

---

4 West "Preventing System Intrusions" in Vacca (ed) *Handbook on Computer and Information Security* (2009) 39; and Hinke, Delugach and Wolf "Protecting Database from Inference Attacks" 1997 16 *Computer & Security* 687.

5 West in Vacca (ed) *Handbook on Computer and Information Security* 39.

6 *Ibid*.

7 Solms "Critical Information Infrastructure Protection – Essential during War Times, or Peace Times or Both?" in Phahlamohlaka, Veerasamy, Leenen and Modise (eds) *IFIP TC9 Proceedings on ICT Uses in Warfare and the Safeguarding of Peace* (2008) 37.

8 Fernandez *Beginning Oracle Database 11g Administration: From Novice to Professional* (2009) 3–5.

9 Hacking is one of the techniques that is employed by criminals to compromise personal or sensitive information stored in a computer system or network. Hacking is actually an act of illegally breaking into other people's computer systems of networks for purposes of soliciting information or data that is stored or reserved in the systems or networks (see Taylor "Hacktivism – In Search of Lost Ethics?" in Wall (ed) *Crime and the Internet* 1ed (2001) 61; and Paget "McAfee's White Paper on Identity Theft" http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf (accessed 2011-07-11).

10 Pharming or spoofing is a "mechanical vandal that creates a fake site masquerading as that of a legitimate provider" in order to steal information or data from unsuspecting persons

In particular, the measures should lessen and/or alleviate the risk of the information or data being used in sabotaging activities, for example, reproduction, adaptation or publication. The foundation for the steps or measures should accordingly be to preserve and safeguard the national security and a sound operation of a state or country. Furthermore, the steps should guarantee that citizens are able to continue their daily activities unhindered.[12]

This article therefore addresses and investigates the challenges of identifying critical databases. In particular, this article offers an approach to address some of these challenges. Before proposing an approach to identifying critical databases it is necessary, this article argues, to examine the regulatory framework of protecting critical databases in South Africa. For the aforementioned reason, this article is structured in the following manner; paragraph 2 deals with the scheme of securing critical databases in South Africa. Chapter IX of the ECT Act is pivotal to the revision of the aforementioned scheme. Furthermore, paragraph 2 reveals the challenges or drawbacks to the approach adopted by South Africa to safeguard critical data and databases. Paragraph 3 investigates the meaning and importance of the risk-based theory of regulation. The rationale for such examination is to argue for the introduction of a method or approach of safeguarding critical databases that promotes the aggregating of foreseen or foreseeable risks and unforeseen or unforeseeable risks. Paragraph 4 of this article presents the conclusion and recommendations. Paragraph 4 of this article particularly sets out the measures that could support South Africa to identify and classify critical data and databases. The measures are influenced by various works undertaken in jurisdictions outside South Africa. However, the measures are a representation or are modelled on the risk-sensitive table contained in Guidance Note 1[13] of the Financial Intelligence Centre (the FIC).[14]

---

and/or disrupts operating businesses (Kapoor *Computerised Banking System in India* 1ed (2008) 16.

11 Various definitions of the crime of phishing diverge. This difference seems to be influenced by the ever-changing nature of contemporary forms of technologies. For example, Myers provides that phishing encompasses social engineering and/or technical attacks (see Myers "Introduction to Phishing" in Jakobsson and Myers (eds) *Phishing and Counter-Measures: Understanding the Increasing Problem of Electronic Identity Theft* (2007) 1–2. The aforementioned attacks are commonly orchestrated by the sending of electronic mails to a web user, falsely claiming to be an established legitimate enterprise in an attempt to scam the web user into surrendering private information that will be used for identity theft (see Granova and Eloff "A Legal Overview of Phishing" 2005 *Computer Fraud and Security* 6).

12 Ndlangisa and Herbst "CII Protection – Lessons for Developing Countries – South Africa as a Case Study" in Rome and Bloomfield (eds) *Critical Information Infrastructure Security: 4th International Workshop, CRITIS 2009* (2010) 168.

13 See the FIC "General Guidance Note Concerning Identification of Clients" https://www.fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf (accessed 2012-05-14) hereinafter "the FIC Guidance Note 1".

14 The FIC was established in terms of section 2 of the Financial Intelligence Centre Act 38 of 2001 (hereinafter "FICA") in February 2002. The FIC has various powers and duties. These powers and duties include, amongst others, to identify proceeds of unlawful activities and to enforce compliance with the provisions of FICA (see s 3(1) read with s 4(c) of FICA).

2 CRITICAL DATABASE PROTECTION

2 1 South African Legislation

Chapter IX of the ECT Act provides measures for the regulating of critical data and databases in South Africa. These data or databases can include data or databases held by public or private bodies or organizations. Critical databases, for purposes of the ECT Act, comprise data that is regarded by the Minister[15] to be of importance to the protection of the national security of the Republic or the economic or social wellbeing of its citizens.[16] The aforementioned data may include, *inter alia*, any data contained in databases regardless of where the data may be accessed, reproduced or extracted.[17] For purposes of Chapter IX of the ECT Act, the Minister must identify critical data and critical databases.[18] The Minister must furthermore require that these data or databases should be registered.[19] Lastly, the Minister must facilitate mechanisms related to the passing of regulations for the management[20] and inspections[21] of critical data and databases. As soon as the critical data and databases have been identified, a critical database administrator (administrator) is therefore required to be appointed.[22] The administrator manages, controls and oversees the functioning of critical databases.[23] The Minister consequently prescribes rules and procedure relating to the manner on which the administrator should manage, control and oversee critical databases.[24]

It is noticeable that South Africa had made an attempt to establish measures to assist the process of identifying critical data and databases. The endeavour was commenced during 2011 by the Department of Communications (Department).[25] More specifically, the Department indicated that it intends embarking on a process of drawing up "an inventory of critical databases".[26] The process was aimed at, amongst others, enabling the Minister to establish and introduce regulations related to the development, maintenance, validity, integrity and security of critical data and databases.[27] However, it is not apparent whether such process was a success and/or whether or not it achieved its intended objectives.

---

15 The Minister within the framework of the ECT refers to the Minister of Communications (see s 1 of the ECT Act).

16 S 1 of the ECT Act.

17 *Ibid.*

18 S 53 of the ECT Act.

19 S 54 of the ECT Act.

20 S 55 of the ECT Act.

21 S 57 of the ECT Act.

22 S 54(2) of the ECT Act.

23 S 1 of the ECT Act.

24 S 5(1) of the ECT Act.

25 South African Government Information "Minister of Communications Starts a Process to Declare Certain Databases as Critical Databases" http://www.info.gov.za/speeches/2003/03111710461002.htm (accessed 2011-10-26).

26 *Ibid.*

27 *Ibid.*

2 2 Identifying critical databases under Chapter IX of the ECT Act

The ECT Act generally grants the Minister wide powers to establish apposite measures to avert attacks on critical data and databases.[28] For example, the Minister can decide on the information or data that should be classified as indispensable to the protection of the national security of South Africa.[29] The Minister can furthermore ascertain and classify the information or data that is fundamental to the security and protection of the economic and social well-being of the South African citizens.[30]

In other circumstances, the Minister has authority to introduce and/or establish rules or procedures for the identification of critical data and databases.[31] The rules or procedures are required to provide for the registration of the full names, address and contact details of the critical database administrator; the location of critical data and databases or their component parts, and the general descriptions of information stored in critical databases.[32] The description of information or data stored in critical databases should, however, exclude the contents of the critical databases.[33] This information or data is required to be maintained by the Department or any other institution established by the Minister for that purpose.[34]

Furthermore, the Department or an institution specified by the Minister must withhold a disclosure of the information subject to certain exceptions.[35] More specifically, the information should be accessible only to the employees of the Department or such institutions.[36] Employees, for purposes of the disclosure, exclude general employees.[37] Therefore, employees for purposes of Chapter IX of the ECT Act include, *inter alia*, the employees that are responsible for the keeping of the register.[38] Furthermore, the rules or procedures should regulate the accessing, transferring and controlling of critical databases; the infrastructural and procedural rules and requirements for securing the integrity of critical databases, and the measures and technological methods to be used in

---

28 See ss 53, 54 and 55 of the ECT Act.

29 S 53(a) of the ECT Act.

30 *Ibid*.

31 S 53(b) of the ECT Act.

32 S 54(2)(a)-(c) of the ECT Act. The recording of these particulars may, however, be waived at the Minister's discretion in terms of s 55(2)(a) and (b) of the ECT Act.

33 S 54(2)(c) of the ECT Act.

34 S 54(2) of the ECT Act.

35 S 56(1) of the ECT Act. The exceptions to the rule that information contained in the register should be kept secret relate to information disclosed to an authority that is investigating a criminal offence or information necessary for purposes of criminal proceedings; information furnished to a government agency responsible for the safety and security of South Africa, information disclosed to a cyber-inspector (s 57 of the ECT Act); information furnished pursuant to section 11 and 30 of the Promotion of Access to Information Act of 2000, or information divulged for purpose of civil proceedings related to critical data and their parts (see generally s 56(2)(a)–(e) of the ECT Act).

36 S 56(1) of the ECT Act.

37 *Ibid*.

38 *Ibid*. The register is therefore maintained by the Department or any other institution or body designated by the Minister for the aforementioned purpose (see s 54(2) of the ECT Act).

storing and archiving critical databases. It is also obligatory that the rules or procedures have measures relating to disaster-recovery plans, and other matters required for the adequate protection, management and control of critical databases.[39]

2 3 Challenges arising out of the Chapter IX provisions

South Africa adopts and implements an incongruous structure to the regulating and protecting of critical data and databases. This structure omits certain essential measures related to the securing and protecting of critical data and databases. The aforesaid measures include, amongst others, the prevention, detection, responding and recovering from attacks to critical data and databases.[40] Importantly, the South African framework fails to provide guidelines setting out the criteria regarding the determination of critical data and databases. The absence of the guidelines therefore raises the fear that the identification of critical data and databases lacks a systematic, scientific and methodological approach. More specifically, there is the danger that critical databases may be selected on a common-knowledge- or known-facts-based approach. The aforementioned approach presumes that it is common knowledge what a critical database is and that the identification of critical data and databases is merely a process of consensus. Furthermore, the common-knowledge approach presumes that the identification of critical data and databases, which are separate concepts in legislation, is the product of common knowledge.

The key problems or dangers with the common-knowledge approach relate to its subjective nature. In particular, the subjective nature of the known-facts-based approach compels the omitting of provisions that encourage the inclusion of a criterion on how critical databases are selected and/or identified. This subjective nature of the common-knowledge approach consequently results in overlooking data and databases that are outside what is generally thought to be critical. By so doing, the subjective nature of the common-knowledge approach fore-grounds certain databases. For example, section 1 of the ECT Act follows an open-ended definition of the terms “critical data” and “critical databases”. The aforementioned therefore leads to the adoption of a one-size-fits-all approach in relation to the security of critical data and databases. This one-size-fits-all-approach presupposes that a singular critical data- and database-regulatory framework is suitable or can be applicable to all scenarios. Furthermore, the one-size-fits-all fails to sufficiently recognize that the general scheme to protect and secure critical data and databases is part of an overall fight against cyber or e-crime.

In response to the abovementioned, this article submits that a regulatory approach analogous to that proposed by Conant and Ashby (the Good

---

[39] S 55(1)(a)–(f) of the ECT Act. For further interesting reading on the powers of the Minister, see generally, s 55(2) of the ECT Act.

[40] See in general OECD “OECD Guidelines for the Security of Information Systems or Networks – Towards a Culture of Security” http://www.oecd.org/dataoecd/16/22/15582260.pdf (accessed on 2012-02-13), hereinafter “OECD Security Guideline”, and the G8 Principles for Protecting Critical Information Infrastructures (adopted by the G8 Justice & Interior Minister) of May 2003 http://www.justice.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf.

Regulatory Theory)[41] is tenable. This approach acknowledges that a suitable and/or fitting framework to control and protect a particular incident or phenomenon is one that is a representation of or modelled from that particular occurrence or phenomenon.[42] Consequently, the Good Regulatory Theory provides that a suitable regulatory framework ought to examine or attempt to examine the dissimilar risks or threats attendant to that occurrence or phenomenon.[43] The regulatory framework that controls the risks or threats is, for purposes of this article, referred to as the risk-based theory of regulating. Paragraph 3 below therefore investigates the nature and meaning of the risk-based theory of regulating. The importance of the risk-based theory of regulating to the general scheme of safeguarding critical data and databases is furthermore exposed.

3 THE RISK-BASED THEORY OF REGULATING

3 1 The nature of the risk-based theory

The risk-based theory is referred to, in fields such as internal auditing, as the risk-management process.[44] Risk management is accordingly a forceful process that seeks to identify, assess, manage, and control potential events or situations.[45] The identification, assessment, management and controlling is made in order to provide reasonable assurance regarding the achievement of particular objectives.[46] Furthermore, risk management depends and/or relies on establishing the source or sources of the risks. The aforementioned relates and extends to identifying, *inter alia*, the type of risks or whether the risks affect a specific event or process.[47] For the above-mentioned reason, risk management enables organizations, and sometimes individuals, to direct organizational and individual resources to high risk cases.

The notion "risk" originates from the Italian verb *risicare*.[48] *Risicare* literally means "to dare".[49] The verb *risicare* is used in the Italian proverb *chi non risica, non rosica* which translates in English into "nothing ventured, nothing gained".[50] Some scholars, particularly, enunciate that the thought or idea of risk was seriously considered during the period of the Italian Renaissance.[51] Throughout the era of the Renaissance, the idea of risk developed as

---

41 See generally Conant and Ashby "Every Good Regulator of a System must be a Model of that System" 1970 1 *International Journal of Systems Science* 89.

42 Conant and Ashby1970 1 *International Journal of Systems Science* 89–91.

43 *Ibid.*

44 Pickett *The Internal Auditing Handbook* 3ed (2010) 175.

45 Griffiths, O'Callaghan and Roach *Internal Relations: The Key Concepts* 2ed (2008) 251.

46 *Ibid.*

47 Pickett *The Internal Auditing Handbook* 179.

48 Deuchars *The International Political Economy of Risk: Rationalism, Calculation and Power* (2004) 7.

49 *Ibid.*

50 Griffiths *et al Internal Relations: The Key Concepts* 251.

51 *Ibid.*

mathematics and gambling sought to "unlock the mysteries of dice throwing".[52]

The structure of the risk-based theory is furthermore comparable to the risk-management framework. For example, the risk-based theory discards a one-size-fits-all approach to regulating. Put differently, the risk-based theory accepts that a holistic and elastic regulatory framework is indispensable. This holistic and elastic regulatory framework focuses on the amount and degree of the risks posed by a particular event. In so doing, the abovementioned framework presupposes that certain facts or circumstances are unknown. Therefore, the unknown facts should, according to the holistic and elastic regulatory framework, be evaluated by means of a risk-assessment-appraisal process.[53] This risk-assessment-appraisal process encompasses, *inter alia*, risk identification, risk classification and risk analysis.[54] The risk-assessment-appraisal process accordingly divorces the idea of relying on "intuition and guesswork" as the basis for assessing risks.[55]

Lastly, the risk-based theory presupposes that a fitting method of regulating facts or circumstances is that which requires an investigation and scrutiny of those relevant facts or circumstances.[56] The aforesaid scrutiny is commonly made by applying measures (preventative or otherwise) notwithstanding the absence of facts to determine the outcome.[57] The foundation for such scrutiny is to strike equilibrium between the taking of the measures and the identification of imminent risks.[58] In other words, a balance should be maintained or sought to be maintained between the amount and extent of the measures and the quantity and degree of the risks. Therefore, in cases where the risks are high, stricter measures to prevent or deter the risks are applied.

3 2 The importance of the risk-based theory

3 2 1 The US approach

The US has responded to the call to apply a risk-based framework to protect its critical databases or infrastructures. It is acknowledged that the risks of attacks to critical databases have become more pervasive in the US in recent times. However, it is conceded that these attacks existed even before the 9/11 US attacks. The US cases of, *inter alia*, *United States v. Robert J. Riggs*, 739 F.Supp. 414 (North District of Illinois. 1990)[59], *United States v.*

---

52 *Ibid.*

53 Zaini, Takim and Endut "Contractor's Strategic Approaches to Risk Assessment Techniques at Project Planning Stage" 2011 *IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA)* 320.

54 *Ibid.*

55 See in general Macaulay "US Critical Infrastructure Interdependency Wheel (CIIW) – Executive Summary" http://www.tysonmacaulay.com/CIIW%20US%20Overview%20-%20July%205%202009.pdf (accessed 2012-05-02).

56 Spedding *Due Diligence and Corporate Governance* (2004) 40.

57 *Ibid.*

58 *Ibid.*

59 Hereinafter "*Riggs*".

Morris, 928 F.2N 504 (2nd Circuit Court 1991) illustrate the abovementioned. For example, the attacks in the Riggs cases were carried out in September 1988. In this instance Riggs and the other accused started a plan to deceive Bell South Telephone Company (company). The company provides telephone services to a number of states in the US.[60] For this reason, the plan was to find entry or access to the company's computer system or networks unlawfully. Afterwards, Riggs and his accomplice would download computer files that contain sensitive and critical information.[61] This is information relating to emergency calls by police, fire, ambulance and other emergency services.[62]

It is argued that Riggs (and similar cases) compelled the US to establish a paradigm which provides for appropriate measures to identify the risks posed by attacks to its critical data and databases. These measures derive their existence from, amongst others, the "National Information Infrastructure" Protection Act of 1996 and sections 121 and 1030 of Titles 6 and 18 of the United States Code (U.S.C.). National Information Infrastructure for purposes of Title 18 of the U.S.C. refers to information related to a government, consumer-credit and/or financial Institutions.[63] Also included here is information obtained by or between governments. The US measures are components of the National Infrastructure Protection Plan (the US Plan).[64] The US Plan depends on a three-fold approach to risk management. This relates to the deterring of risks, the mitigating of the vulnerabilities and the minimizing of the consequences.[65] For example, it is essential to identify and assess the nature and scope of the risks; to detect the threat posed by the risks, and to study those threats with a view to understand the actual or potential attacks to critical databases.[66] The US Plan encourages the building, managing, refining and improving of comprehensive inventories of the assets systems and networks that make up the US's National critical infrastructure and key resources (CIKR).[67] The US Plan furthermore sets out, amongst others, various methods to be used to alleviate the risks to critical data and databases.[68] The methods include, *inter alia*, improving security and reducing systematic interruptions and alteration caused by passive and active attacks.[69]

---

60 *United States v. Robert J. Riggs*, 739 F.Supp. 414 (North District of Illinois. 1990) 45–46.

61 *Riggs* 45–46.

62 *Ibid*.

63 Doyle "Cybercrime – A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Law" 2008 *Congress Research Service* 2.

64 See in general Homeland Security "National Infrastructure Protection Plan – Partnering to Enhance Protection and Resilience" http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed 2012-05-17).

65 S 121(1)–(9) of the U.S.C. For further interesting reading see, the US Office of the Press Secretary "Presidential Proclamation – Critical Infrastructure Protection and Resilience Month, 2012" http://www.whitehouse.gov/the-press-office/2012/11/30/presidential-proclamation-critical-infrastructure-protection-and-resilie (accessed 2013-02-27).

66 S 121(1)(a)–(c).

67 See Homeland Security in fn 64 above.

68 *Ibid*.

69 Zhang, Ou, Singhal and Homer "An Empirical Study of a Vulnerability Metric Aggregation Method" http://csrc.nist.gov/staff/Singhal/xou-anoop-workshop2011-paper.pdf (accessed on 2012-08-10).

The measures and/or methods that are contained in the US Plan have led to the establishing of the US Critical Infrastructure Interdependency Wheel (CIIW).[70] The CIIW acknowledges the interconnectedness of recent ICTs. Therefore, the CIIW recognizes that an attack to a particular data or database is, given this interconnectedness, likely to have adverse effects on other data or database(s).[71] Furthermore, the CIIW encourages the establishing of a framework to identify and classify divergent risks to the overall US critical infrastructure. Accordingly, the CIIW uses a wheel as an aid to the identification and aggregation of the various risks and their impact on critical data and databases.[72] The basis for such reliance is to determine whether or not a singular attack can be said to be limited to a single data or database.[73] The CIIW therefore concludes that indeterminate risks to a particular data or database commonly cascade or extend to or impinge on other data and databases.[74]

3 2 2 The UK approach

The UK approach to secure critical data or databases is part of the overall UK Strategy to Secure Information Society.[75] It is argued that this strategy is a representation of the "Global Plan of Action" on the information society.[76] For example, it is recognized that attacks to critical data and databases adversely affect the realization of this information society.[77] The aforementioned has therefore led some academics to label modern ICTs, and their complexity and interconnectedness as constituting an enemy of the Information of the information society.[78] The aforementioned is linked to the idea that it has nowadays become impossible to separate systems and networks.[79] Consequently, an activity which is carried out on one system or network can be accessed or is accessible on other systems or networks.[80]

Furthermore, the UK acknowledges, amongst others, that a one-size-fits-all approach to identify and classify information is untenable.[81] For example, it is recognized that some information is critical than other. The significance

---

70 See Homeland Security in fn 64 above, 78.

71 *Ibid.*

72 *Ibid.*

73 See Macaulay in fn 55 above.

74 *Ibid.*

75 See, Commission of the European Communities "A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment" http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf (accessed 2013-02-26).

76 The "Global Action Plan" on the information society was introduced following the World Summit on the information society which was held in Geneva during 2003.

77 See Commission of the European Communities in fn 75 above.

78 Van Eeten, Roe, Schulman and de Bruijne "The Enemy Within – System Complexity and Organisational Surprises" in Dunn and Mayer (eds) *International CIIP Handbook 2006: Analysing Issues, Challenges and Prospects* (2006) 89–109.

79 Cavelty "Critical Information Infrastructure – Vulnerabilities, Threats and Responses" http://www.unidir.ch/pdf/articles/pdf-art2643.pdf (accessed 2013-04-27).

80 *Ibid.*

81 Centre for the Protection of National Infrastructure "Protection against Terrorism" http://www.cpni.gov.uk/documents/publications/2010/2010002-protecting_against_terrorism_3rd_edition.pdf (accessed 2013-02-25).

of information depends on the nature and quality of such information. However, the interconnected nature of modern technologies leads to a singular attack or risk of attack to a critical data or database (direct attacks) being felt by other critical data or databases (indirect attacks). For this reason, the UK established a Critical Information Infrastructure Protection Action Plan (the CIIP).[82] The CIIP seeks to reinforce the security of critical databases.[83] Furthermore, the CIIP aims to enable the UK to, *inter alia*, prepare, prevent, detect and respond, mitigate and recover from attacks directed to its critical databases.[84] Consequently, a framework is established which denounces the idea that the impact of a direct attack should be confined to a targeted critical data or database.[85]

3 2 3 The South African approach

South Africa recognizes the importance of the risk-based theory only in limited cases. For example, South Africa acknowledges that the risk-based theory is essential when preventing, *inter alia*, other social crimes, for example, money-laundering and terrorism. On the one hand, money-laundering is often associated with dirty or hot money.[86] The dirtiness or hotness of money is mostly linked to the assiduous manner in which the money is obtained.[87] For the abovementioned reason, money laundering encompasses, amongst others, the concealment of illegal money or assets so that the money or assets can appear to be legal or to be obtained by legal means.[88] Conversely, terrorism comprises a total sum of activities or non-activities that result in adverse consequences to the society.[89] For example, terrorism denotes any act or conduct which directly or indirectly causes death or serious bodily injury to an inhabitant or any other person and that is intended to intimidate a population, or to compel a government or an international organization to carry out or to abstain from carrying out any act.[90]

The risk-based theory, for purposes of anti-money laundering and anti-terrorism, encourages the performing of rigorous due diligence in certain cases. This thorough due diligence is normally carried out to persons or transactions posing a high risk of money-laundering or terrorism. This can be demonstrated by means of an example: a person (B) was convicted by

---

82 See the European Commission "Achievements and Next Steps – Towards Global Cyber-Security" http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:ET:PDF (accessed 2013-02-26).

83 *Ibid*.

84 *Ibid*.

85 See Centre for the Protection of National Infrastructure in fn 81 above.

86 Rider "Taking the Profit Out of Crime" in Rider and Ashe (eds) *Money Laundering Control* (1996) 4; and Van Jaarsveld "Mimicking Sisyphus? – An Evaluation of the Know Your Customer Policy" 2006 27 *Obiter* 230–232.

87 Bond and Thornton "Money Laundering" 1994 324 *Accountants Digest* 6–7.

88 See s 1 of FICA; Madinger *Money Laundering: A Guide for Criminal Investigators* 2ed (2006) 6; and Levi *Federal Money Laundering Regulation: Banking, Corporate, and Compliance* (2003) 1–3.

89 S 1 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004.

90 See in general Part 1 and 2 of Chapter 2 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act.

country C of drug-trafficking. At the time of his conviction B had a property business. B wishes to invest all his monies in country D. B therefore visits Bank E situated in country D with the aim of opening a cheque account. Bank E is required to perform CDD measures as part of its customer-acceptance policies. However, the measures of due diligence should be extensive. Put differently, Bank E must investigate B's source of funds and whether or not the monies originate from the proceeds of drug-trafficking. It is, however, noticeable that the extensive measures applied to B may be waived in cases where the risks are low. For example, A works for B Municipality and receives a monthly salary of R3 500.00. A therefore visits Bank E with a view to open a savings account.[91] The object of the account is to receive and keep A's salary deposited at the end of each month. In this case, Bank E should perform simplified due-diligence measures. These measures can be said, according to A and Bank E's relationship, to be equivalent to the risks posed to Bank E. Thus, in the latter scenario, the risk-based theory can be viewed as a method to mitigate the time and costs of CDD measures performed to A. In particular, the aforesaid theory allows Bank E to give priority to transactions that pose high risks of money-laundering or terrorism. Therefore, Bank E can provide less attention (simplified due diligence) to low-risk transactions.

For the abovementioned reason, financial institutions (FIs) apply the risk-based theory as part of their duty to prevent money-laundering and terrorism.[92] The aforementioned duty is protected and regulated under the customer due-diligence (CDD) process.[93] In undertaking the CDD process, for example, FIs carry out a methodical practice.[94] This practice necessitates an appraisal of personal information or data.[95] The assessment is made in order to classify the various risks posed to an anticipated relationship.[96] The aim of such an assessment is to ensure that the actions of a person conform to an FI's policies, procedures and methodologies.[97] For example, the FIC Guidance Note 1 requires FIs to exercise value judgment when undertaking the CDD process.[98] This value-judgment encourages the dismissing of a common-knowledge approach or an approach founded on box-ticking.[99] Consequently, the FIC recommends the adoption of an approach risk to a singular FI which may also have adverse consequences to a number of

---

91 In South Africa, the aforementioned accounts are referred to as the Mzansi Accounts. Mzansi Accounts were launched during August 2004 to cater for the previously disadvantaged population of South Africa that was financially excluded in the past (see Bankable Frontier Associates "South African Financial Diaries and the Mzansi Initiative – Five Years Later" http://www.bankablefrontier.com/assets/pdfs/BFA%20Mzansi%20Financial% 20Diaries%20revisits%20160210%20FINAL.pdf (accessed 2011-10-31).

92 S 21 FICA.

93 The CDD process encourages the identification and establishing of a person and the verification of a person's personal particulars. The identification and verification is required to commence before a person establishes a business relationship or concludes a transaction or single or occasional transaction with a business (FI) (see in general s 21 of FICA).

94 *Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* 1992 (1) All SA 411 (A) 413–416.

95 See s 21(1) of FICA.

96 *Indac Electronics Ltd v Volkskas Bank Ltd* supra 413–416.

97 Spedding *Due Diligence and Corporate Governance* 3.

98 The FIC Guidance Note 1.

99 *Ibid*.

FIs.[100] Therefore, the FIC establishes a method of assessing the threats that focuses on the "risk indicators".[101] The abovementioned method differentiates, amongst others, between different risks carried in or outside the borders of South Africa and risks posed by foreign and South African citizens.[102] Accordingly, the risks are averaged (rolling average) in order to establish the extent and degree of the risks.[103] The purpose of this value judgment is to assist FIs to employ measures that are commensurate with the "nature of the risk" involved in a particular situation.[104]

Furthermore, the CDD process acknowledges that different risks commonly exist. For example, risks may be posed by a person; the relationship that a person has with an FI or the type of transaction or transactions concluded.[105] Therefore, FIs must create and establish a risk matrix or profile. The matrix or profile generally eases a process of classifying the type of person, the type of relationship and the type of transaction or transactions.[106] Owing to the vastness of transactions, Emergency System Alerts (ESAs) monitored by Computer Emergency and Response Teams (CERTs) are developed. These CERTs must be composed of trained professionals.[107] These experts must investigate and provide information on present and future attacks or risks to critical data or databases.[108] Thus, the CERTs must be structured in a manner that allows them to assist in the monitoring, warning, alerting and carrying out of critical data- or database-recovery measures.[109]

3 3 Commentary on the risk-based framework to secure critical databases

The US and UK approaches to safeguard critical data and databases are explicit in relation to need for risk-based frameworks. More specifically, these approaches support the view that a proactive critical data- and database-security framework should be developed.[110] Put differently, the US and UK approaches recognize the importance of a process to systematically

---

100 Within the framework of FICA, these FIs are referred to as Accountable Institutions (see s 21 of FICA) and are listed under Schedule 1 of FICA.

101 The FIC Guidance Note 1.

102 *Ibid*.

103 *Ibid*.

104 *Ibid*.

105 The Financial Action Task Force (FATF) "Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures" http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf (accessed 2010-05-10). For further interesting reading see, par 5.3 of the United Kingdom's (the UK) Core Guidance to the Money Laundering Regulations of 2007.

106 Pieth "The Wolfberg Process" in Muller, Kälin and Goldsmith (eds) *Anti-Money Laundering: International Law and Practice* (2007) 97.

107 Rittinghouse and Hancock *Cybersecurity Operations Handbook* (2003) 327.

108 *Ibid*.

109 See OECD "OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security" http://www.oecd.org/dataoecd/16/22/15582260.pdf (accessed 2012-03-12).

110 See Zhang, Ou, Singhal and Homer in fn 69 above.

assess the risks of attacks to critical data and databases.[111] It is argued that these approaches are in line with the guidelines set out by the Organisation for Economic Co-operation and Development's (the OECD).[112] In particular, the OECD requires that a paradigm to secure critical data and databases must encourage the adoption of the risk-based theory as part of its structure.[113] Accordingly, various methods of undertaking the risk-based theory should be established. For example, apposite awareness of the risks to critical data and databases may be created.[114] The aim of such awareness creation must be to dispense knowledge and experience regarding the development of policies and practices to secure critical data and databases.[115] Furthermore, the measures to prevent attacks to critical data and databases by outside intruders (anti-intruder measures) should be established. The measures should facilitate the enhancing of the security of the entire information system or network. Therefore, the measures must hearten or encourage the carrying out of a risk-assessment or -appraisal process. The aforementioned processes must encompass a suitable examination of the vulnerabilities and risks to critical data and critical databases.[116] Put differently, the risk-assessment processes must help to determine the degree and level of the risks.[117] More specifically, external factors, such as technology, physical and human factors, policies and third-party services with security implications must be considered.[118] The aforementioned considerations should lead to the ongoing or periodic reviewing of the adopted structure of the risk-based theory.[119]

South Africa also recognizes the importance of risk-sensitive based frameworks in certain selected cases. In particular, South Africa considers the risk-based paradigms as fundamental to preventing crimes such as money-laundering and terrorism. However, this importance is omitted from the approach that South Africa takes in relation to safeguarding critical data and databases.

4 CONCLUSION

This article argues that South Africa has made great progress in providing for the control of attacks to critical data and databases. For example, South Africa has passed legislations that cover the measures against attacks or threats of attacks to critical data and databases. The ECT Act is an example of those legislations. In particular, Chapter IX of the ECT Act set out the manner and structure of critical data- and databases-protection paradigm in South Africa. However, it is argued that the Chapter IX measures are founded on a stagnant or inflexible critical data- or database-regulatory

111 *Ibid.*
112 See OECD in fn 109 above.
113 *Ibid.*
114 *Ibid.*
115 OECD "OECD Recommendation of the Council on the Protection of Critical Information Infrastructures" http://www.oecd.org/dataoecd/1/13/40825404.pdf (accessed 2012-01-23).
116 *Ibid.*
117 *Ibid.*
118 See OECD Security Guidelines in fn 109 above.
119 *Ibid.*

framework. For example, the measures continue from the premise that an attack or risk of attack to a particular data or database can only be confined to that data or database. For this reason, Chapter IX of the ECT Act promotes a framework to identify critical data and databases that is based on a common-knowledge. The abovementioned viewpoint is founded on the premise that a process to identify and classify critical data and databases is a product of guesswork. Therefore, an approach that is applied to identify and classify one data or database is or can also be applicable to identify and classify other data or databases.

For the aforementioned reason, this article recommends that South Africa follows the US and UK approaches to critical data and database protection as the lead. In particular, it is essential for Chapter IX of the ECT Act to recognize that the systems where data and databases are kept are interconnected. Therefore, a structure to identify and classify critical data and databases must recognize that risks to data and databases are borderless in nature. For this reason, a framework to regulate critical data and databases should extend beyond a single data or database. More specifically, such a structure should concede to the fact that contemporary technologies (that is, the Internet and the Web) facilitate the connection of databases online. Consequently, a critical data- or database-regulatory framework that is flexible and adaptable to the technological innovations is essential.[120] The abovementioned framework must generally be modelled from the technology itself[121] and its effectiveness should be monitored by skilled CERTs.

This article concedes that regulations and/or directives can provide swift, efficient and effective response to the issues and/or ambiguities that are identified above. It is, however, essential that any regulatory initiative in the aforementioned regard should also involve the affected institutions (those which keep critical data).

[120] Conant and Ashby1970 1 *International Journal of Systems Science* 89–91.
[121] *Ibid.*