Journal of Contemporary Management
Volume 11

Strategic information security management as a key tool in enhancing competitive advantage in South Africa

V NAIDOO (University of KwaZulu-Natal)

B VAN NIEKERK (University of KwaZulu-Natal)

Abstract
In the current business environment there is a high chance of an information security incident occurring, largely due to the ever-increasing reliance on information technologies. This threat is resulting in a change in legislature regarding the protection of information. Measures and procedures therefore need to be implemented at a strategic level within an organisation to counter the information security threats. The paper descirbes various components of strategic management of information security with an emphasis on the South African context, and disucsses how effective strategic information security and a corporate culture of information security will enhance competitive advantage in the South African and global business environments.

Key phrases
competitive advantage, corporate culture, information security culture, information security strategy

1. INTRODUCTION

Strategic competitive advantage lies at the heart of an organisation's long term sustainability and growth. Executive management together with all the other levels of management and its employees should be charged with maintaining high levels of financial performance by gaining an edge over its rivals in the market place. A way forward for the organisations is to have in place proper strategy for information security to prevent security incidents and cyber-attacks. This means developing strategy to safeguard the organisations competitive strengths, capability, knowledge, personnel, and capital resources. In recent years huge multinational companies such as Coca-Cola (Robertson 2012: Internet), Google (McMillan 2010: Internet), Global Payments (Information Security Media Group 2013: Internet) and the information security solutions provider, RSA, which is reported to have led to attempt hacks on a number of defence industries using their SecurID security system (Poulsen 2011: Internet), have been hard hit by cyber-attacks.

In some cases, this may have left the company vulnerable to their rival competitors. These companies were also exposed to financial losses, public relations disasters and a heightened media frenzy that has led to their brand image and credibility in the marketplace being damaged. For example, the aftermath of the Global Payments breach is estimated at costing $94 million (Information Security Media Group 2013: Internet).

No organisation should be exposed to such IT security breaches as it has the potential to lower their market share in that industry, expose them their competitors and damage their reputation and good standing in the industry. To overcome such dire circumstances, management should prepare their organisations against exposing their companies to such cyber-attacks by developing and implementing new information security strategies.

Von Solms and van Niekerk (2013: 101) investigate the use of the terms information security and cyber security, and conclude that the terms are not identical and should not be used interchangeably. For the purposes of this paper, we will consider cyber-security as a subset of information security, where information security will cover cyber, physical, psychological, and organisational aspects.

Section 2 will provide the literature and highlight the repercussions of information security breaches occurring within the organisation. Thereafter Section 3 explores management strategies to protect against internal and external cyber-attacks. Section 4 discusses the relationship between information security and competitive advantage, and Section 5 concludes the paper.

2. LITERATURE

A number of South African organisations have fallen victim to information security incidents, which have resulted in significant financial loss. South African Airways suffered an estimated 14 million Rand loss due to a credit card fraud conducted by internal staff and a crime syndicate in 2006 (Rondganger 2007: Internet). A corrupt employee of Vodacom, a mobile telecommunications network, aided a crime syndicate in intercepting one-time pins used by online banking websites in 2009, which resulted in them stealing approximately 7.7 million Rand (van Rooyen 2009: Internet). In December 2010 hackers with possible insider help stole 8 million Rand from Land Bank, however most of it was recovered (Potgieter 2011: Internet).

Approximately 42 million Rand was stolen from Postbank in January 2012 when hackers accessed an internal computer that was linked to the main server (Swart & Afrika 2012:

Internet). In November 2012 PayGate, a South African payment processing organisation, was breached compromising hundreds of thousands of credit cards (Arde 2012:17). Cyber-crime in South Africa is estimated to have a 3.7 billion Rand impact the national economy in terms of direct costs, and a further 6.5 billion Rand in terms of indirect costs (Symantec Corporation 2012: Internet).

There are four frameworks and legislative areas that relate to information technology in South Africa, listed in no particular order:

- The King III Report (2009);
- The Electronic Communications and Transmissions Act (2005);
- The Regulation of Interceptions of Communications Act (2002); and
- The Protection of Personal Information Act (2013).

The King III Report (King Committee 2009:2) was developed to serve as a blueprint for how South African businesses should operate within the realm of good corporate governance. According to Hough and Arthur (2011:320) IT governance is dealt with in detail in the King III Report, whereas previous versions did not address IT governance or security (King 2009:26). The report suggests that in exercising their duty of care, directors should ensure that prudent and reasonable steps be taken within the organisation with regards to IT governance. The King III Report is the South African equivalent of Sarbanes-Oxley Act in the United States (King 2009:26).

The Electronic Communications and Transmissions Act (ECT 2005:2) provides basic regulations for all forms of communications via electronic and transmitted media.

The Regulation of the Interception of Communication Act (RICA 2002:2) requires anyone providing electronic communication services to make provision to provide legal intercepts of that information. It also restricts under what conditions, and what the legal requirements are, for such intercepts. These two laws may have significant implications for organisational strategic management, as entire business processes may need to be altered in order to remain compliant to these new laws. Organisations will also need to be more proactive about information security, rather than reactive.

The Protection of Personal Information Act (POPI 2013:2) governs how organisations use and process personal information and require protection of such information.

Compliance with the above legislation is merely doing the minimum to make sure the relevant 'check boxes' are marked. Being compliant may provide the organisation and the

management with some protection should an incident occur. However, there still needs to be an expensive investigation process and the brand image may still suffer due to the breach. Therefore, doing the minimum to remain compliant is not sufficient. Strategically, an organisation should do more than the minimum compliance as this will provide some legal standing that efforts were made to prevent security breaches should an incident occur, and will help mitigate the chances of the breach occurring in the first place.

Gaines, Hoover, Foxx, Matuszek and Morrison (2012:2) indicate that managers must not only understand the role of information security in corporate governance and corporate strategy formulation, but they must also understand how the accepted norms are changing over time. The threat environment is changing rapidly and previously undiscovered vulnerabilities come to light or new vulnerabilities are inadvertently introduced regularly. Consequently there is a need to regularly review information security measures and strategies to ensure that they are suitable for the current and future operating environment.

2.1 Alignment with a company's competitive advantage

According to Hough and Arthur (2011:6-7) when an organisation is embarking on a sustainable competitive advantage it should focus on any of the four strategic approaches listed below:

- Cost-based competitive advantage over rivals, where the aim is to be the low-cost provider in that industry.
- Differentiating features such as higher quality, broader product range, higher performance, value-added services, more attractive styling, technological superiority, or exceptional value for money.
- Narrow focus on niche markets and winning a competitive edge by doing a better job than rivals of serving special needs and tastes of buyers comprising the niche.
- Developing expertise and resource strengths that give the organisation competitive capabilities that rivals cannot match with capabilities of their own.

Thompson, Strickland and Gamble (2006:6) suggest that in established industries, most organisations recognise that having a durable advantage over competitors' is based more on building competitively valuable expertise and capabilities than it does on having a unique or distinctive service or product. Particularly in the finance and investment sector, a publicly visible security culture will provide investors and customers with a sense of confidence in the services which can often be the defining factor in them choosing your service over a

competitor's. What set Lockheed Martin aside from other companies after the RSA SecurID breach was their unique cyber-security system which successfully prevented the attackers from achieving their goals (Higgins 2013: Internet).

Daneshvar and Ramesh (2010:1-2) argue that organisations are aware of the capacity of IT to build sustainable competitive advantages, and the special effects, benefits and implications of IT in improving business efficiency and performance. In keeping with the above argument, the authors has expanded on this by indicating that managing information system security within an organisation is crucial in maintaining competitive advantage through the use of its IT.

Porter (1996:72) goes on further to add that IT has affected competition as follows:

- The organisation structure changes, which alters the rules of competition;
- Organisations have new opportunities to outperform their rivals, giving them a competitive advantage;
- The existing operations of organisations can spawn whole new businesses.

As IT evolves, it continues to change the way companies do business. Recent evolutions such as social media, cloud computing, and the increased pervasiveness of smartphones provide both opportunities and risks; the impact on corporate security is one of the major concerns in adopting these technologies.

2.2 Possible repercussions if IT security is breached within the organisation

The most obvious repercussions of an information security breach will be loss of funds if the organisation accounts were targeted and loss of productivity during the recovery phase and while the security incident is investigated. This often adds indirect costs, as staff will be idle but on full pay during system cleansing and there will be costs associated with the investigation and any possibly legal action. In certain countries legislature also imposes a fine if there is a breach of personal information. In South Arica, the Protection of Personal Information Act (POPI 2013:100) imposes an administration fine of up to R10 million for a breach of personal information. This will also affect efficiency and service delivery as normal business process will be pushed aside in order to prioritise recovery from the breach. Some attacks will intentionally target websites in order to prevent legitimate users from accessing the services.

Breaches will result in a public relations issue, where the organisation needs to communicate with affected stakeholders, and others not directly affected but who will be understandably

concerned. Regardless, of the efforts of the public relations group, there will most likely be some devaluation of the corporate brand, and probably some loss of market segment due to existing clients leaving and potential clients being deterred.

Depending on the nature of the security incident, there will be legal implications for the organisation and management. The most severe will be where an organisation has failed to prevent fraud or protect personal or sensitive information. In South Africa public organisations are expected to be compliant with the King III Report guidelines, which places executive management as the accountable party (King Committee 2009:16). The Control Objectives for IT 5 framework (COBIT5) developed by ISACA also lists the executive and chief information security officer as the accountable party for many processes, including security and continuity (ISACA 2012:186,192). This may result in responsible parties trying to shift blame, resulting in internal conflict between managers and departments, which may ultimately result in further animosity and a reduction in staff morale if not controlled.

The financial and legal implications, loss of market share, internal conflict and damage to corporate branding will ultimately result in a negative impact on the organisation's competitive advantage. In order to protect an organisation from this fate, there are a number of management strategies to promote a corporate culture of information security, and to mitigate incidents from occurring. These will be discussed in detail in the next section.

3. MANAGEMENT STRATEGIES TO PROTECT AGAINST INTERNAL AND EXTERNAL INFORMATION SECURITY ISSUES

This section describes the various strategies that can be employed to mitigate information security risks. These generally form a layered approach, with a focus on people, processes, and technology.

3.1 Training staff to circumvent the breaches

Staff members need to be trained on information security incidences. Staff also need to be briefed on how to not incur security breaches. They need to be shown how to identify possible incidents and what procedures to follow thereafter. Swanepoel, Erasmus and Schenk (2008:445) strongly suggest that although well thought-out strategies and efficient human resources planning, recruitment and selection initially provide the organisation with the required employees, additional training is normally necessary to provide them with job-specific skills which enable them to survive over time.

3.2 Managing staff effectively by enhancing accountability

Mitnick and Simon (2002:3) argue that employees are the greatest threat to information security, whether through negligence or intentionally, but most usually due to a lack of knowledge. They believe that if staff members are managed effectively, that is there is proper screening of staff before they are employed, then these background checks would be able to identify only the best candidate for the job. Secondly if proper segregation of duties are in place then staff would be directly accountable and will guard the organisations information security in a more efficient and prudent manner. Segregation of duties also splits the accountability for each step in a process, thereby reducing the possibility of collusion to conduct illegal activities such as fraud.

3.3 Developing policies in IT to safeguard the organisation

By having proper policy in place management and staff can have a guideline present on how to think and take decisions within the organisation. Pearce and Robinson (2007:304) argue that "policies communicate guidelines to decisions. They are designed to control decisions while defining allowable discretion within which operational personnel can execute business activities." According to Brotby (2009:121), "management of information security will be primarily concerned with strategic business outcomes, ensuring that security activities properly support the organisation's objectives and alignment with the overall business strategy". Overall policy compliance is imperative. This means that proper policies in IT to safeguard the organisation need to be developed. Amoroso (2013:122) comments that the “question is not whether to develop a security policy, but rather what the policy will entail.”

These IT security policies should be aligned to all the goals and objectives at all three management levels within the organisation. These IT policies would form the building blocks that guides the organisation in information and IT security issues that permeate the organisation. By having written policy in place management and employee commitment and responsibility to uphold the goals and objectives of the organisation will be further strengthened.

3.4 Promoting good leadership

Leadership is the corner stone of any organisation’s success. In particular, leadership in key areas can influence the strengthening of a company's competitive advantage. Thompson, Strickland and Gamble (2006:289) cite Maxwell (2002) as stating that success is within reach of every organisation, but the amount of success is dependent on the leadership

ability reflected in the organisation. The higher an organisation wants to climb in terms of success, the more it needs its leaders and the greater the amount of influence needed from these individuals. In order to achieve synergy within the organisation, good leaders are required that motivate their employees to align their departmental goals and objectives with the overall security information culture. This entails leaders motivating their staff to be more security conscious.

Information security starts with the organisation's leadership. As mentioned in Section 2.2, the executive can be considered accountable and responsible for many processes. Not only does the organisation's leadership need to show support for any information security initiatives that are to be implemented, but they need to be seen to follow the same secure procedures and policies as all other employees. Not only will this encourage employees to accept the security initiatives, but also senior leadership is often the target of attacks against an organisation's information security. However, an incorrect emphasis on responsibility and leadership may result in erratic behaviour which could result in breaches (ISACA 2013b:40). Therefore, a fine balance needs to be struck whereby leadership encourages secure behaviour without forcing such behaviour that the organisation becomes dysfunctional.

3.5 Instilling a corporate culture that encompasses information security

Management should have policies, corporate culture and good corporate governance in place so that good ethical behaviour permeates all levels of the organisation. Thompson, Strickland and Gamble (2006:293) argue that the taproot of corporate culture is the organisations values, beliefs and business principles that set forth how its affairs ought to be conducted. Within the organisation management needs to include IT security management as part of their sub-culture. This entails that information security within all levels of management should be part of their everyday duties and responsibilities. In order to ensure the desired user behaviour, it is necessary to cultivate an organisation sub-culture of information security (Schlienger & Teufel 2003:3; Von Solms 2000:618). This culture, the behaviour, and ethics are an important enabler to risk management and thus corporate information security (ISACA, 2013a:41-42).

According to Thompson, Strickland and Gamble (2006:293) Enron's collapse in 2001 was partly the product of a flawed corporate culture. Enron became unglued because a few top executives chose unethical and illegal paths to pursue corporate revenues and profitability targets. It was these executives whose arrogance, greed, ego and deliberate obscure

accounting practices and an end-justifies-the-means mentality collapsed a once successful and productive organisation.

Similarly, a flawed corporate culture may increase risk regarding cyber-security. In particular, ignoring individual awareness in favour of organisation-wide governance and control may result in a possible breach or security incident not being recognised and too much trust can be exploited in a social context to conduct an attack (ISACA 2013b:37). Human aspects of culture may also increase risk, such as tending towards convenience over security or habits result in lack of improvement in enterprise information security (ISACA 2013b:40).

A strong corporate culture of security does not necessarily indicate a closed authoritative management style that avoids all risk, but rather the ideal culture can integrate healthy risk awareness with creativity and an acceptance of new technologies (Amoroso 2013:124). A corporate culture that instils secure behaviour may take years to develop, however having business processes and procedures that results in secure behaviour will aid drastically (Amoroso 2013:124-125). Such procedures will include the aspects of segregation of duties described in Section 3.2. As mentioned in Section 3.4 the senior leadership of an organisation need to be seen actively following the security policies, therefore the security culture must encompass all levels of the organisation.

3.6 Organisational conflict should be managed if a security breach occurs

If and when IT breaches occur within the organisation proper steps should be taken by management to manage organisation conflict. If not managed properly, conflict can disrupt the tasks, objectives and goals within the organisation, impact on productivity and cause demoralization amongst staff.

According to Mensah and Naidoo (2013:56) conflict can divert efforts and energy from productive endeavours to wasteful feuds. Energy could be put to productive use if proactive actions are taken to prevent wasteful conflicts. Prevention of such conflicts would require that steps be taken to turn the known causes of such conflicts – communication failures; biases; differences in personalities, energy, and motivation; dissatisfaction with remuneration; causes of delays; etc. (Kloppenborg 2009:363) – into preventive measure through anticipation, setting of ground rules, and early reaction to symptoms.

An established corporate culture will determine the level of involvement of different staff categories in recovery from a breach (ISACA & Ernst & Young, 2013:75), enabling each of

the involved staff members or departments to clearly understand their roles and responsibilities.

3.7 Public relations has a role to reinforce public perception if a security breach occurs

According to Payne (1993:159) public relations (PR) is "concerned with a number of marketing tasks that includes building or maintaining image, supporting the other communication activities, handling problems and issues, reinforcing positioning, influencing specific publics and assisting the launch of new services". If there is an IT security breach PR has to work around the clock to appease aggrieved stakeholders of the organisation who fear that this IT breach can destroy the organisation's profit margins and future sustainability.

According to Elgin, Lawrence and Riley (2012: Internet) Coca-Cola never publicly disclosed a series of corporate IT system breaches, some were also kept secret from shareholders and senior executives. This included sensitive information on the proposed multi-billion Dollar takeover of Huiyuan, which collapsed a few days later. Some may say by not disclosing that their IT security system was breached would be their way of good PR. However, in South Africa the King III report clearly compels organisations to be transparent, and many laws insist the public notification of breaches when personal information has potentially been compromised.

3.8 Budgeting for information security

As with other important strategic initiatives, management should budget for information security. If and when breaches do occur they then would be covered via insurance or other financial reserves to secure the company’s assets and competitive capabilities. Since information security breaches can cost the organisation millions of Rand, budgeting for such incidences should be essential. According to Information Security Media Group (2013: Internet) the data breach Global Payments revealed in April 2012 had cost the company $93.9 million.

4. INFORMATION SECURITY AND COMPETITIVE ADVANTAGE

Information security is about safeguarding the assets, intellectual capital and capabilities of a business. Van Niekerk and Von Solms (2006:2) reiterates this by arguing that in today’s world most organisations need information systems to "survive and prosper." Since information has become a highly valuable asset to modern organisations today, information security needs to be put in place to ensure that this asset is properly secure and used by

employees and management of the organisation only. Therefore managing information security becomes an organisation's competitive advantage, since this is the only system if properly utilized that can safeguard and protect all the assets and intellectual capital of the organisation.

The evolving IT environment continuously results in new opportunities and challenges for organisations. At the forefront of the concerns is the impact new technologies will have on corporate IT security. For example, mobile phones can be easily lost or stolen, and employees may access email with sensitive information using the email functions; this constitutes a breach of security. By effectively addressing and managing the information security concerns of new technologies enables corporations to leverage them to create new opportunities and increase their value-added services and consequently their competitive advantage over their rivals.

A holistic view of information security management needs to be implemented: this includes creating a corporate ethos of security through the business processes, policies, and awareness training. This will enable the acceptance of the relevant IT security controls at an operational level, and also provide the ability to respond quickly and efficiently to any incident. Not only should there be compliance with the relevant South African legislation and frameworks such as King III, RICA, and POPI, but additional international best practices should also be embraced to further protect the organisation.

A strategic information security committee, whilst obviously having representatives from IT, risk management, and auditing, should also have representatives from human resources and corporate relations. This ensures that there is an alignment with human resources in terms of required background checks and awareness training, but human resources can also report any disgruntled employees or unusual behaviour which may indicate a possible insider security threat. Corporate relations should report any external complaints or controversial issues that may be facing the organisation, as these indicate that there is an increased likelihood that an attack on the organisation's information systems may be used as a form of protest.

Should the organisation's security management be successful, potential new business opportunities may arise in the form of consulting and providing their expertise to other companies. This may provide a distinct advantage over competitors, whose similar security projects may not have been as successful or failed. Successful strategic information security

programs will mitigate losses and bad publicity due to breaches, provide product differentiation, and place the company as a leader through their expertise.

5. CONCLUSION

Given the current IT environment where security breaches are becoming the norm and significant financial losses are incurred, increasing attention is being drawn to the governance and protection of personal information and other information assets. It is essential for organisations to implement strategic management over their information security. This includes processes and policies, technologies, and awareness of the employees. It is essential that these be fully implemented and supported at a strategic level for it to be effective throughout the organisation structure. Management need to safeguard the organisation's personal information competitive strengths, capability, know-how and human and capital resources. In order to achieve this they need at their disposal proper policy, technology and training to safeguard their management information systems. This would result in enhancing their competitive advantage and maintain their growth and long term sustainability in industry.

REFERENCES

AMOROSO EG. 2013. Cyber attacks: protecting national infrastructure. Student edition. Waltham, MA: Butterworth-Heinemann.

ARDE A. 2012. Hack attack a costly lesson for banks. *The Independent on Saturday*. 17, Column 1, 17 November.

BROTBY WK. 2009. Information security management metrics: a definitive guide to effective security monitoring and measurement. Boca Raton, FL: Auerbach.

DANESHVAR P & RAMESH HN. 2010. Information technology and corporate strategies in small and medium enterprises. *International Journal of Management & Strategy* 1(1):1-16, July-Dec.

ECT see **REPUBLIC OF SOUTH AFRICA**.

ELGIN B, LAWRENCE D & RILEY M. 2012. Coke gets hacked and doesn't tell anyone. Bloomberg. 5 November. [Internet: http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html; downloaded on 2013-03-07.]

GAINES C, HOOVER D, FOXX W, MATUSZEK T & MORRISON R. 2012. Information systems as a strategic partner in organisational performance. *Journal of Management and Marketing Research* 10(1):1-17. [Internet: http://ww.w.aabri.com/manuscripts/11997.pdf; downloaded on 2013-03-26.]

HIGGINS KJ. 2013. How Lockheed Martin's 'Kill Chain' stopped SecurID attack. *Dark Reading*. 12 February. [Internet: http://www.darkreading.com/authentication/167901072/security/attacks-breaches/240148399/how-lock-heed-martin-s-kill-chain-stopped-securid-attack.html; downloaded on 2013-02-13.]

HOUGH J & ARTHUR A. 2011. Crafting and executing strategy creating sustainable high performance in Southern African businesses. 2nd ed. London: McGraw Hill.

INFORMATION SECURITY MEDIA GROUP. 2013. Global payments breach tab: $94 million. Bankinforsecurity.com. 10 January. [Internet: http://www.bankinfosecurity.com/global-payments-breach-tab-94-million-a-5415/op-1; downloaded on 2013-01-14.]

ISACA. 2012. COBIT 5 Enabling processes. Rolling Hills, Il: ISACA.

ISACA. 2013a. COBIT 5 for risk. Rolling Hills, Il: ISACA.

ISACA. 2013b. Transforming cybersecurity using COBIT 5. Rolling Hills, Il: ISACA.

ISACA & ERNST & YOUNG. 2013. Responding to targeted cyberattacks. Rolling Hills, Il: ISACA.

KING M. 2009. King III: A new corporate playing field. *Enterprise Risk* 3(9):25-27 [Internet: http://reference.sabinet.co.za/webx/access/electronic_journals/sh_eprise/sh_eprise_v3_n9_a14.pdf; downloaded on 2013-03-27].

KING COMMITTEE. 2009. King report on governance for South Africa. Johannesburg: Institute of Directors in Southern Africa.

KLOPPENBORG TJ. 2009. Project management: a contemporary approach. International student edition. Melbourne: South-Western Cengage Learning.

MAXWELL JC. 2002. The 21 irrefutable laws of leadership: follow them and people will follow you. Nashville, TN: Thomas Nelson.

MCMILLAN R. 2010. China: Google attack part of a widespread spying effort. *MacWorld.* 13 January. [Internet: http://www.macworld.co.uk/digitallifestyle/news/index.cfm?newsid=28293; downloaded on 2010-01-20.]

MENSAH SN & NAIDOO V. 2013. Management issues in the implementation of development projects for employment creation in Lesotho. *Journal of Contemporary Management* 2(1):48-58.

MITNICK K & SIMON W. 2002. The art of deception: controlling the human element of security. London: Wiley.

PAYNE A. 1993. The essence of service marketing. London: Prentice Hall.

PEARCE JR & ROBINSON RB. 2007. Strategic management formulation, implementation and control. 10th ed. McGraw Hill: London.

POPI see **REPUBLIC OF SOUTH AFRICA.**

PORTER ME. 1996. How information gives you competitive advantage. In AUSTER E & CHOO CW (eds). Managing information for the competitive edge. New York: Neal-Schuman. pp. 71-92.

POTGIETER D. 2011. Absa intercepts Land Bank swindle. *Saturday Star*. 8 January [Internet: http://www.iol.co.za/business/companies/absa-intercepts-land-bank-swindle-1.1009423; downloaded on 2012-09-11.]

POULSEN K. 2011. Second defence contractor L-3 'actively targeted' with RSA SecurID hacks. Wired.com Threatlevel. 31 May. [Internet: http://www.wired.com/threatlevel/2011/05/l-3/; downloaded on 2011-06-06.]

REPUBLIC OF SOUTH AFRICA. 2002. Regulation of Interception of Communications and Provision of Communication-Related Information Act. (RICA). Act 70 of 2002. Pretoria: Government Printer.

REPUBLIC OF SOUTH AFRICA. 2005. Electronic Communications and Transmissions Act (ECT). Act 36 of 2002. Pretoria: Government Printer.

REPUBLIC OF SOUTH AFRICA. 2009. Protection of Personal Information Act (POPI). Act 4 of 2013. Pretoria: Government Printer.

RICA see **REPUBLIC OF SOUTH AFRICA**.

ROBERTSON J. 2012. How a Coca-Cola exec fell for a hacker's e-mail trick. Bloomberg. 6 November. [Internet: http://go.bloomberg.com/tech-blog/2012-11-06-how-a-coca-cola-exec-fell-for-a-hackers-e-mail-trick/; downloaded on 2012-11-23.]

RONDGANGER L. 2007. Credit card scam costs SAA R14m. *IOL News*. 10 May. [Internet: http://www.iol.co.za/news/south-africa/credit-card-scam-costs-saa-r14m-1.352307; downloaded on 2012-09-11.]

SCHLIENGER T & TEUFEL S. 2003. Information security culture - from analysis to change. *3rd Annual Information Security South African Conference*. Sandton, 1-13, 9-11 July.

SWANEPOEL BJ, ERASMUS BJ & SCHENK HW. 2008. South African human resource management theory & practice. 4th ed. Lansdown: Juta.

SWART W & AFRIKA M. 2012. It was a happy New Year's day for a gang who pulled off...R42m Postbank heist. *The Sunday Times Live*. 15 January. [Internet: http://www.timeslive.co.za/local/2012/01/15/it-was-a-happy-new-year-s-day-for-gang-who-pulled-off...r42m-postbank-heist; downloaded on 2012-01-15.]

SYMANTEC CORPORATION. 2012. Norton cybercrime report. [Internet: http://za.norton.com/cybercrime report/promo?inid=uk_hho_downloads_home_link_cybercrimereport; downloaded on 2012-09-12.]

THOMPSON JR, STRICKLAND AJ & GAMBLE JE. 2006. Strategy: core concepts, analytical tools, readings. 2nd ed. Boston: McGraw Hill.

VAN NIEKERK J & VON SOLMS R. 2006. Understanding information security culture: a conceptual framework. *6th Annual Information Security South African Conference*. Sandton, 1-10, 5-7 July.

VAN ROOYEN K. 2009. Hidden price of a banking scam. *The Sunday Times*. 18 July. [Internet: http://www.thetimes.co.za/PrintArticle.aspx?ID=1036132; downloaded on 2009-07-30.]

VON SOLMS SH. 2000. Information security - the third wave. *Computers & Security* 19(7): 615-620.

VON SOLMS R & VAN NIEKERK J. 2013. From information security to cyber security. *Computers & Security* 38(1): 98-102.