Interdisciplinary Journal of Information, Knowledge, and Management Volume 11, 2016

Cite as: Irons, A., & Ophoff, J. (2016). Aspects of digital forensics in South Africa. *Interdisciplinary Journal of Information, Knowledge, and Management, 11,* 273-283. Retrieved from http://www.informingscience.org/Publications/3576

Aspects of Digital Forensics in South Africa

Alastair Irons
University of Sunderland,
Sunderland, United Kingdom

alastair.irons@sunderland.ac.uk

Jacques Ophoff
University of Cape Town,
Cape Town, South Africa

jacques.ophoff@uct.za

Abstract

This paper explores the issues facing digital forensics in South Africa. It examines particular cyber threats and cyber threat levels for South Africa and the challenges in addressing the cybercrimes in the country through digital forensics. The paper paints a picture of the cybercrime threats facing South Africa and argues for the need to develop a skill base in digital forensics in order to counter the threats through detection of cybercrime, by analyzing cybercrime reports, consideration of current legislation, and an analysis of computer forensics course provision in South African universities. The paper argues that there is a need to develop digital forensics skills in South Africa through university programs, in addition to associated training courses. The intention in this paper is to promote debate and discussion in order to identify the cyber threats to South Africa and to encourage the development of a framework to counter the threats – through legislation, high tech law enforcement structures and protocols, digital forensics education, digital forensics skills development, and a public and business awareness of cybercrime threats.

Keywords: digital forensics, cybercrime, legislation, skills development, South Africa

Introduction

This paper presents a review of the computer forensics (predominately forensics focused on PCs and laptops) and digital forensics (forensics from all digital artefacts, including mobile phones, smart phones, tablets, GPS devices, embedded systems) environment in South Africa. In the paper the authors consider the development and evolution of cybercrime and cyber threats, government legislation in the cyber domain, and academic response (research, course provision) in South Africa in order to illustrate the environment for digital forensics in the country.

This paper is motivated by the perceived need to address the skills gap in digital forensics investigations. South Africa faces numerous challenges related to cybercrime and cyber threats, thus making the ability to investigate such incidents essential. The Norton Cybercrime Report suggested that over 1 million South Africans were victims of cybercrime in 2012.This is due to the lack of cyber security awareness from individuals and organizations and the steps needed to protect their digital artefacts, data and information (Symantec, 2013).

The continued exponential growth in the availability and use of computer and digital technology in transactions and interactions (in South Africa but also across the African continent) in business, industry and social media lead to huge volumes of data in the virtual world. The growth in the use of computing

Editor: Rajeev Manhas
Submitted: April 27, 2016: Revised: July 31, 2016, September 8 & 28, 2016; Accepted: October 7, 2016

and digital devices has not been matched by a raising of public awareness of the threat of cybercrime or the use of cyber security to promote safe digital activities. Growth in the number of Internet users in South Africa (from 5 million in 2008 to 26.8 million in 2015, representing almost 50% of the population) and the number of people using mobile Wi-Fi (Stork, Calandro, & Gamage, 2014) to access the Internet means that there is an increase in the potential threat from cybercrime. In a report on cybercrime McAfee (2014) suggests that "once a country gets Broadband there is a spike in cybercrime" (p. 6) and the spike is exacerbated when connectivity is via mobile Wi-Fi. In addition to the growth in Internet access there is a growth of related technologies including cloud computing, mobile technologies, unsecured Wi-Fi, social media, and geopositional data. The changing and expanding digital environment means that the amount of data in the virtual world and the type of data that may be of 'interest' to cyber criminals presents an evolving and developing set of challenges for digital investigations and for digital forensic investigators. Simultaneously the ubiquitous nature of computing and digital technology means that potentially every 'traditional' crime, in addition to every cybercrime, has a possible digital investigation aspect to it. Any crime that has a digital artefact associated with it potentially requires a digital forensics investigation that needs to be carried out by investigators with appropriate digital forensics training and competence.

Because all data is potentially of interest in cybercrime investigations there is an unprecedented challenge for law enforcement agencies. There is a need for highly skilled digital forensics investigators to meet the demand and address the challenges facing digital investigations as well as addressing the threat to society. It is argued in this paper that, in order to meet the skills shortage and gap in digital forensics in South Africa and address the growing need for highly skilled digital investigators, there is a need to review provision of digital and computer forensics degree programs available in the country.

The paper proceeds with an overview of the research methodology used. It then moves on to review the impact of cybercrime in South Africa, followed by specialized cybercrime legislation. Next the requirements for developing digital forensic skills and capabilities are discussed, followed by a review of the state of forensic teaching provision at universities in South Africa. A summary of the findings follows, along with recommendations to address the issues identified. Finally, the conclusion summarizes the main points in the paper.

Methodology

The purpose of this paper is to provide background to the environment of cybercrime, computer forensics, and digital forensics in South Africa. In order to develop the South African picture an examination of the current reports on cybercrime and related legislation is required. In addition the provision of opportunities for higher skills development in computer forensics and digital forensics needs to be determined. In order to understand these areas a number of steps were taken.

First an examination of the reports on cybercrime in South Africa was undertaken. The feedback from the reports is provided in the next section of this paper. Whilst the examination of the reports gives a perspective on cybercrime, and there is a suggestion from the figures that the economic impact is significant, there is no way of knowing whether this is a complete picture. Often such reports represent a small proportion of cybercrime that is reported and categorized. The UK's Office of National Statistics (2015) report on cybercrime suggests that the level of reported cybercrime is 'the tip of the iceberg' and there is no reason to indicate that the completeness of reporting is any better in South Africa.

Second, the methodology applied in this paper focused on a review of the existing legislation in South Africa to address cybercrime. The findings suggest that, although there is a level of rele-

vant legislation, there is a need to ensure that legislation keeps pace with the development of cybercrime opportunities and the rise in levels of cybercrime.

The third part of the applied methodology was to undertake a systematic analysis of program provision in South African universities. This was done through a detailed search of university websites looking for computer forensics and digital forensics course availability. The following points detail the process that was followed:

- To initiate the systematic analysis a list of South African universities, as providers of higher education, was compiled.
- Next, a search of each university's website was undertaken to examine the programs offered. The search spanned all university programs and used a set of relevant keywords: computer forensics, digital forensics, forensics, forensic, cybercrime, digital crime, computer crime, computer security, and cyber security. This provided an indication of programs in computer forensics, digital forensics, forensic science, or digital investigation.
- For resulting programs a further sub-search was conducted at curriculum level to identify the content of programs (i.e., course details) and whether computer forensics or digital forensics was covered. Valid results were verified by both authors.
- In addition to the above, a drill-down analysis of computer science modules in South African universities offering this degree was undertaken to determine whether the topics of computer forensics or digital forensics were addressed. Due to the technical nature of the content there is often a link between these areas.

The findings from the systematic analysis of programs are provided in Table 1 in this paper.

Cybercrime in South Africa

There has been a significant global growth in cybercrime over the last 10 years and South Africa has not been exempt from this. Symantec (2013) estimates that 70% of South Africans have been victims of cybercrime in one form or another. Two of the most common threats users face are phishing attacks and Sim-swap fraud. The South African Minister of Telecommunications and Postal Services, Siyabonga Cwele, said in parliament that around 32% of small and medium enterprises in South Africa run the risk to fall bait to cyber and phishing attacks (Peyper, 2016).

McAfee's (2014) research, undertaken on behalf of the Center for Strategic and International Studies (CSIS), indicates that cybercrime has a significant impact on the South African economy with an estimated R5.8 billion (£325million sterling) lost each year. Cybercrime cost to the economy is likely to increase year-on-year and be equivalent to almost 0.2% of the country's GDP. This is similar in percentage terms to the UK (0.2%) but lower than USA (0.64%) and Germany (1.6%) according to McAfee. Irrespective of GDP percentage, the figure of R5.8 billion remains a significant amount of finance. It should be noted that it is notoriously difficult to get an accurate figure on the amount and value of cybercrime because of a lack of reporting, poor detection, and variable classification.

Alfreds (2014) focuses on ID Theft as one particular variant of cybercrime and estimates that "it costs this country (South Africa) in excess of R3 billion per annum in ID theft just from a governmental perspective". If there is R3 billion per annum lost to ID theft as one particular instance of cybercrime it would suggest that when all aspects of cybercrime are taken into account that R5.8 billion is an underestimate. The Department of Justice and Constitutional Development produced the draft version of the Cybercrimes and Cybersecurity Bill (2015) and estimated that the cyber-related offences were escalating and currently increasing at a rate that exceeded a value in excess of R1 billion annually. The variations in cost of cybercrime from the above examples illus-

trate how difficult it is to get a true value on the cost of cybercrime to the economy or the number of people affected. Whatever the type of cybercrime, source, or measure it is apparent that there is a significant issue.

Symantec (2013) ranked South Africa third highest (behind China and Russia) by number of cybercrime victims and put the annual cost of cybercrime at $0.3 billion USD. It is also estimated that more adults (up to 80%) in emerging markets are victims of cybercrime, compared to developed markets. One of the key reasons for this is the lack of security awareness, both amongst individuals in society and in business organizations (Labuschagne, Eloff, Veerasamy, Leenen, & Mujinga, 2011).

Cybercrime is a growing concern in South Africa, as evidenced by a PwC (2014) report stating that "69% of South African respondents indicated that they had been subjected to some form of economic crime in the 24 months preceding the survey, compared to 37% of global respondents" (p. 5). Common threats include mobile and financial malware, advanced persistent threats, and web threats. Threats commonly spread via removable devices and local networks (Kaspersky Lab, 2014). The rise in mobile malware are a potential concern to both individuals and companies alike, seeing as bring your own device (BYOD) vulnerabilities are still largely unmanaged in South African organizations (Cisco, 2014). In addition, according to Microsoft (2014, pp. 101-102), South Africa is host to a higher than average concentration of phishing sites and report high rates of phishing impressions. The top services being targeted by criminals include Internet banking, e-commerce and social media (Wolfpack, 2013, p. 36).

Computer crime has been on the research agenda since Stander, Dunnet, and Rizzo (2009) completed a small-scale survey of South African organizations. In their study the occurrence of electronic attacks were reported by 45 percent of respondents. However, the reporting of cybercrime incidents and resulting losses is inconsistent, especially in the SME sector (Bougaardt & Kyobe, 2011). Further exploration of South Africa's cyber security status has continued. Recent work by Swart, Irwin, and Grobler (2014) tests an experimental design to measure South African information security metrics at a national level. Initial results are promising and could inform cyber security and cybercrime policy requirements.

Understanding the online activities of school learners and investigating initiatives to improve online safety is an important and recent focus (e.g., Kritzinger, 2014; Kritzinger & Padayachee, 2013; Walaza, Loock, & Kritzinger, 2014). This includes educating children about online risks and protection mechanisms within the national school curriculum. Understanding the most significant online risks is important – an example is the rising problem of cyber bullying in South African schools (Kritzinger, 2014). Building blocks to address cybercrime at school level have been proposed, catering for specific challenges faced in South Africa (Walaza et al., 2014). Key to this is engaging key role-players to create an e-safety culture (Kritzinger & Padayachee, 2013).

Preventing, detecting, and resolving cybercrime in South Africa is proving problematic. Survey data indicates that there is a perceived shortage of digital forensics skills, especially in the government sector (Wolfpack, 2013, p. 50). Key issues related to government initiatives and skills development need to be addressed; those specifically relevant to computer forensics include (Wolfpack, 2013, pp. 7-8):

- The lack of a functional national Computer Security Incident Response Team (CSIRT) – this situation is considered in the action plan at the end of this paper.
- A shortage of experienced computer forensics, incident handlers and secure software coding skills – discussed in the section on educational provision.
- A need to invest in training and skills development across all sectors, with a focus on deeper investigative and prosecutorial skills.

- Selective training relevant police constables with basic cybercrime skills on how to identify, categorize, and open a docket for cybercrime incidents.

Initiatives to address these issues are already underway and should reduce South Africa's vulnerability to cyber threats. However, there needs to be a clear strategy to address the issues, with clearly articulated outputs and closely monitored targets. It is suggested in this paper that there is an opportunity to develop a uniform set of protocols and guidelines for the South African context for detection, search, seizure, acquisition, evidential integrity, and evidential continuity – drawing on United Kingdom (UK) ACPO and United States (US) FBI standards. Any protocols should be developed collaboratively, for example with the South African Computer Security Incident Response Team (CSIRT).

Cybercrime Legislation in South Africa

The question of how to address cybercrime within South Africa, and the broader continent, is a significant challenge, but there has been initial progress in addressing this. The introduction of specialized cyber legislation is seen as a positive step forward (Cassim, 2011). Legislation is also crucial to allow effective investigation of cybercrimes – a case in point being the definition of 'cyber inspectors' by the Electronic Communications and Transactions (ECT) Act (2002), according to Snail (2009). However, an all-inclusive and consistent approach across the African continent is required, developing legislation which applies nationally and internationally. At this point in time existing legislation does not provide this, which is a potential weakness in trying to address cybercrime.

Legislation in South Africa for dealing with cybercrime centers on the Criminal Procedure Act (1977) and the ECT Act (2002). The ECT Act was designed to detect and prosecute cybercriminals and to provide a national response to the more serious incidents of cybercrime. However, these pieces of legislation by their very nature are not able to deal with or manage the current cyber environment and, thus, the current levels and types of cybercrime. There is a need to consistently review and update appropriate legislation in order to deal with the changing and evolving nature of cybercrime.

The ECT Act (2002) also encourages collaboration between agencies in South Africa and overseas – particularly the US. The contention behind collaboration is to improve and develop the specialist skills and capabilities of digital investigators. However as is argued in this paper, in addition to international collaboration, there is a need to develop a skilled digital investigation and computer forensics workforce through programs of education and training of those who are living and working in South Africa.

Developing Digital Forensics Skills and Capabilities in South Africa

In order to develop appropriate digital investigations skills and create a highly trained technical and professional capacity to address the growing issue of cybercrime in South Africa, it is suggested in this paper that there is a need to develop university programs that will produce graduates with relevant skills, knowledge, and experience. Rogers (2003), in discussing the US environment, points out that a professional certification in computer forensics is currently lacking a 'gold standard'. In the UK Irons, Stephens, and Ferguson (2009) argue that there is a minimum curriculum coverage that is required in order to have a computer forensics program. In undergraduate programs that coverage should be implemented throughout the program, developing fundamental knowledge and principles in early years then specializing in the final year of the program. In the South African context this would mean specialization at Honours year with underpinning computer forensics knowledge being studied in years 1 to 3 of the undergraduate syl-

labus. A computer forensics program should have a balance of theoretical and practical learning. In the UK context Irons et al. (2009) suggest that the following topics should be include (but not be limited to):

- the definition of digital investigation principles, processes, and procedures including theory and practice in detection, search, seizure, and acquisition;
- investigation standards and guidelines;
- the nature of digital evidence and the technical expectations and challenges of dealing with digital evidence;
- the underpinning computer forensics principles of evidential continuity and evidential integrity, in the securing, recovering, and analyzing of digital evidence;
- technical expertise in using computer forensics applications, software, and programs; and
- the particular professional and ethical issues and challenges facing a computer forensics practitioner.

Whilst it is possible to train graduates from subjects such as Computer Science in the packages and procedures of computer forensics, those graduates are likely to lack the requisite, specialist, depth of knowledge and skill that comes from an academic program specifically designed to produce a computer forensics practitioner or specialist.

In addition to the theoretical aspects of a computer forensics program, there is a need for a strong practical and applied side of the syllabus. This will require case material for students to work on and appropriate laboratory facilities to develop the practical and hands on skills. It is likely (based on experience in the UK) that computer forensics laboratories need to be designed in such a way that they do not interfere with the standard operation of a university's computing resource, i.e., the computer forensics lab should be a stand-alone facility (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003). Inevitably this has a capital cost associated with it. In addition there is an expectation in the UK that graduates leave university with applied knowledge of standard forensic software such as EnCase and FTK (GCHQ, 2015). Again there is a significant cost, in terms of licensing, for a university to take into account for these products.

A number of universities in South Africa offer courses in forensics science, forensic accounting, forensics auditing, forensic psychology and computer law, and a number of courses that consider the principles of forensic investigations. However, there are very few courses that specialize in computer forensics, and those that include an element of computer forensics usually have this attached as optional choices or single modules to other programs such as Computer Science or Information Systems.

There is a small amount of digital forensics teaching provision on degree programs at South African universities with a number of programs including modules in digital or computer forensics. For example, 'Introduction to Digital Forensics' as a module on the Certificate in Cyber Security at the University of Johannesburg (2016); University of Pretoria's (2016) module on 'Digital Forensics and Investigation'; and a module on 'Computer Forensics' as part of the Postgraduate Diploma in Management Information Systems at the University of Cape Town (2016a). One of the authors has provided an Honours course on the Computer Science program at UCT as a visiting scholar since 2014 (University of Cape Town, 2016b). North-West University (2016) offers a range of short course in the forensic domain including one on 'Commercial Forensic Information Technology' with the prospect of creating a full program in the future. The University of the Western Cape (2016) suggests that students graduating from its B.Com. (Information Systems)

program have career opportunities as "computer forensics specialists", but the focus in the curriculum is on forensic accountancy rather than on computer forensics.

Whilst these provide thorough introductions to principles in digital forensics there is not the space in any of the examples to cover the breadth and depth required to develop computer forensics professionals that a full Honours program or a specialist Master's program in digital forensics would provide.

Table 1summarizes the computer/digital forensics provision in South African Universities and illustrates the lack of specific computer forensics or digital forensics courses in South Africa. In order to address the skills gap and tackle the issues of cybercrime in South Africa it is suggested that there is a need for specialist programs either at undergraduate, Honours or post-graduate levels.

Table 1: Computer/digital forensics programs in South African Universities

University	Honours			Postgraduate		
	Coverage	Module	Program	Coverage	Module	Program
University of Cape Town	✓	✓	x	✓	✓	x
University of Fort Hare	x	x	x	x	x	x
University of Free State	x	x	x	x	x	x
University of KwaZulu-Natal	x	x	x	x	x	x
University of Limpopo	x	x	x	x	x	x
North-West University	x	x	x	x	x	x
University of Pretoria	✓	✓	x	x	x	x
Rhodes University	x	x	x	x	x	x
University of Stellenbosch	x	x	x	x	x	x
University of Western Cape	✓	x	x	x	x	x
University of the Witwatersrand	x	x	x	x	x	x
University of Johannesburg	✓	✓	x	✓	✓	x
Nelson Mandela Metropolitan University	x	x	x	x	x	x
University of South Africa	x	x	x	x	x	x
University of Venda	x	x	x	x	x	x
Walter Sisulu University	x	x	x	x	x	x
University of Zululand	x	x	x	x	x	x
Cape Peninsula University of Technology	x	x	x	x	x	x
Central University of Technology	x	x	x	x	x	x
Mangosuthu University of Technology	x	x	x	x	x	x
Tshwane University of Technology	x	x	x	x	x	x
Vaal University of Technology	x	x	x	x	x	x

A few universities (Cape Town, Johannesburg, and Pretoria) offer Honours modules in computer/digital forensics, and the University of the Western Cape has some coverage of forensics in other modules. These modules cover a wide range of topics in computer forensics both in terms of theory and practice, and it is encouraging to see inclusion of computer forensics in Honours

programs in computer science. However the current provision are small courses and do not allow students to develop knowledge and understanding of computer forensics in enough breadth and depth to enable graduates form these programs to directly enter professional roles in the forensics domain. Similarly at Master's level the inclusion of computer forensics currently is mainly included as part of programs in cyber security. Whilst the development of computer forensics skills and knowledge will enhance the skills of a cyber security professional, again there is lack of requisite knowledge and depth in order to provide graduates for computer forensics roles after graduation.

There is an opportunity to collaborate with UK Higher Education Institutions in developing an appropriate body of knowledge and supporting curricula at undergraduate and postgraduate level. This could build on existing programs while increasing the depth and breadth of digital forensics higher education offers.

Findings

The various cybercrime reports that are available (discussed earlier in the paper), the development of technology, and the growing global threat from cybercrime suggest that the level of cybercrime and the various types of cybercrime are likely to grow in South Africa. The reliance on mobile networks in South Africa for efficient digital access increases the cybercrime threat, when compared to countries that have a more secure broadband infrastructure.

The growing threat from cybercrime should be met with robust legislation and an appropriate computer forensics and digital forensics skills set to counter cybercrime. The findings in this paper suggest that neither is the case currently in South Africa.

There is a need for specific legislation to address the threats and consequences of cybercrime. Part of this legislation will need to define the admissibility and authenticity of digital evidence in South Africa. The current legislation goes some way to provide an environment to enable the submission of digital evidence from computer forensics and digital forensics investigations. However, the legislation needs to evolve to reflect the development of computing devices and computing technologies.

In order to address the resolution of cybercrime there is the need to develop a suitably skilled workforce. The analysis of courses on computer forensics and digital forensics in South Africa suggests that there is insufficient in-depth provision and that there is a need to consider increasing the level of provision.

Taking the Challenge Forward

In order to address the issues put forward in this paper and to put in place suggestions and recommendations for discussion and debate the following action plan is proposed as a way to address the opportunities and challenges facing computer and digital forensics in South Africa.

- The development of frameworks to counter the threats from cybercrime by creating a uniform set of protocols and guidelines for the South African context for detection, search, seizure, acquisition, evidential integrity, evidential continuity (for example, drawing on UK (ACPO) and US (FBI) standards on handling and investigation digital evidence) and to collaborate in the development of contextualized guidelines with South African agencies such as the CSIRT.
- Create an education program to address the skills gap in computer and digital forensics. The program should include University programs, training programs, and a suite of Continued Professional Development (CPD) courses for professionals currently working in

cyber security, traditional police investigations, and other government agencies. At university level it is suggested that consideration be given to Honours program, specifically on computer and digital forensics, drawing on the body of knowledge developed in education programs in other parts of the world. It is suggested in this paper that there is an opportunity to utilize the UK body of knowledge to help in developing curriculum in the South African context.

- Encourage collaboration between government agencies, South African private digital forensics providers, and academia to enhance the digital forensics provision in South Africa and increase the capacity in dealing with the threat of cybercrime.
- Further research to include the cyber security environment and impact this has on cybercrime, legislative issues, and employability in digital forensics.

Conclusions

The purpose of this paper was to examine aspects of the current position of computer and digital forensics in South Africa, to encourage debate and discussion, and to suggest an action plan to address educational and skills development needs in the discipline in South Africa.

As access to computing and computing technology grows and as the use of computing resources and applications becomes even more widespread, the potential threat of cybercrime also grows. In order to develop counter measures to cybercrime there is a need to raise awareness of the threats from cybercrime and the cost of cybercrime. In addition there is also the need to put in place policy frameworks that will allow for digital investigations to be undertaken. The final part in the jigsaw is to address the skills gap in digital forensics and to establish programs of study, training, and continued professional development programs that will enable digital investigations to take place.

This paper presents the digital crime environment in South Africa, and the findings are preliminary. As indicated at the outset it is hoped that the issues raised in this paper generate debate and discussion. Further work is planned to examine a number of issues: firstly, the state of cyber security in South Africa; secondly, the employment position in digital investigations in South Africa; and finally, a review of the legislative infrastructure in the digital ecosystem in South Africa.

References

Alfreds, D. (2014). *Top cybercrime threats for 2015*. Retrieved from http://www.fin24.com/Tech/News/Top-cybercrime-threats-for-2015-20141205

Bougaardt, G. & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. *The Electronic Journal of Information Systems Evaluation, 14*(2), 167–178.

Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: Evaluating measures adopted by South Africa and other regional role players. *The Comparative and International Law Journal of Southern Africa, 44*(1), 123–138.

Cisco. (2014). *Cisco South African BYOD research highlights that many organisations in South Africa are still vulnerable when it comes to security* [Press release]. Retrieved from http://www.cisco.com/web/ZA/press/2014/082514.html

Criminal Procedure Act. (1977). *Criminal Procedure Act, Act 51 of 1977*. Retrieved from http://www.gov.za/sites/www.gov.za/files/Act%2051%20of%201977s.pdf

Cybercrimes and Cybersecurity Bill. (2015). *Cybercrimes and Cybersecurity Bill Draft for Public Comment*. Retrieved from http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf

Electronic Communications and Transactions Act. (2002). *Electronic Communications and Transactions Act, Act 25 of 2002*. Retrieved from http://www.gov.za/sites/www.gov.za/files/a25-02.pdf

GCHQ. (2015). *Certification of Master's Degrees in Digital Forensics*. Retrieved from https://www.cesg.gov.uk/articles/gchq-certification-master-s-degrees-cyber-security

Irons, A., Stephens, P., & Ferguson, I. (2009). Digital investigations as a distinct discipline: A pedagogic perspective. *Digital Investigation, 6*(3), 65–71.

Kaspersky Lab. (2014). *Kaspersky Lab reports on cyber threats in Africa in the first quarter of 2014* [Press release]. Retrieved from http://www.kaspersky.co.za/about/news/virus/2014/Kaspersky_Lab_reports_on_cyber_threats_in_Africa_in_the_first_quarter_of_2014

Kritzinger, E. (2014). Online safety in South Africa - A cause for growing concern. *Proceedings of the 2014 Information Security for South Africa Conference, Johannesburg, South Africa*, (pp. 1–7).

Kritzinger, E., & Padayachee, K. (2013). Engendering an e-safety awareness culture within the South African context. *Proceedings of the 2013 AFRICON Conference, Pointe-Aux-Piments, Mauritius*, (pp. 1–5).

Labuschagne, W., Eloff, M., Veerasamy, N., Leenen, L., & Mujinga, M. (2011). Design of a cyber security awareness campaign for internet café users in rural areas. *Proceedings of the 2011 IFIP TC9/TC11 South African Cyber Security Awareness Workshop, Gaborone, Botswana*.

McAfee. (2014). *Net losses: Estimating the global cost of cybercrime*. Retrieved from http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf

Microsoft. (2014). *Microsoft security intelligence report (Volume 17)*. Redmond, WA: Microsoft Corporation.

North-West University. (2016). *Short courses presented by the NWU Programme in Forensic Accountancy*. Retrieved from http://pbs.nwu.ac.za/img/uploads/file/Forensic/2016/short%20course%20for%20forensic%20accounting.pdf

Office of National Statistics. (2015). *Improving the reporting of cybercrime*. Retrieved from http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html

Peyper, L. (2016). *32% of SMEs in SA at risk of cyber-attacks – Cwele*. Retrieved from http://www.fin24.com/Economy/32-of-smes-in-sa-at-risk-of-cyber-attacks-cwele-20160309

PwC. (2014). *Global economic crime survey*. Sunninghill: PricewaterhouseCoopers.

Rogers, M. (2003). Computer forensics: Science or fad. *Security Wire Digest, 5*(55).

Snail, S. (2009). Cyber crime in South Africa – Hacking, cracking, and other unlawful online activities. *Journal of Information, Law and Technology, 2009*(1). Retrieved from http://go.warwick.ac.uk/jilt/2009_1/snail

Stander, A., Dunnet, A., & Rizzo, J. (2009). A survey of computer crime and security in South Africa. *Proceedings of the 2009 Information Security for South Africa Conference, Johannesburg, South Africa*, (pp. 1–10).

Stork, C., Calandro, E., & Gamage, R. (2014). The future of broadband in Africa, *Info, 16*(1), 76–93.

Swart, I., Irwin, B., & Grobler, M. (2014). Towards a platform to visualize the state of South Africa's information security. *Proceedings of the 2014 Information Security for South Africa Conference, Johannesburg, South Africa*, (pp. 1–8).

Symantec. (2013). *Norton cybercrime report*. Mountain View, CA: Symantec Corporation.

University of Cape Town. (2016a). *Computer forensics*. Retrieved from http://www.commerce.uct.ac.za/InformationSystems/CourseInfo/INF4016W

University of Cape Town. (2016b). *Digital forensics*. Retrieved from https://www.cs.uct.ac.za/teaching/honours/Honours%20Handbook%202016v11.pdf

University of Johannesburg. (2016). *Certificate in cyber security*. Retrieved from http://adam.uj.ac.za/csi/Courses.html

University of Pretoria. (2016). *Digital forensics and investigations*. Retrieved from http://www.cs.up.ac.za/courses/COS783

University of the Western Cape. (2016). *EMS specialised programmes*. Retrieved from https://www.uwc.ac.za/Faculties/EMS/Pages/EMS-SPECIALISED-PROGRAMMES.aspx

Walaza, M., Loock, M., & Kritzinger, E. (2014). A framework to integrate ICT security awareness into the South African schooling system. *Proceedings of the 2014 Southern African Institute for Computer Scientist and Information Technologists Conference, Pretoria, South Africa,* (pp. 11-18). New York, NY: Association for Computing Machinery.

Wolfpack. (2013). *The South African cyber threat barometer (2012/13)*. Johannesburg: Wolfpack Information Risk.

Yasinsac, A., Erbacher, R., Marks, D., Pollitt, M., & Sommer, P. (2003). Computer forensics education. *IEEE Security &Privacy, 1*(4), 15–23.

Biography

Alastair Irons is a Professor of Computer Science in the Department of Computing, Engineering and Technology (CET) at the University of Sunderland – where his subject interests focus on computer forensics and cyber security. From 2008 to 2014 he was Head of Department in CET. Prior to joining the University in September 2008 he worked at ONE North East, Northumbria University and ICI, having moved to the north east from Scotland after graduating in 1984 from Edinburgh University. Alastair became a National Teaching Fellow in 2010. He is a visiting scholar at the University of Cape Town in South Africa. He serves on the management board of DYNAMO, the management board of Digital Leaders North East, the Advisory Board of the North East Digital Catapult and on the management board of the North East Fraud Forum, is chair of the BCS Academic Accreditation Committee, sits on the BCS Academy Board, is chair of the BCS Cybercrime Forensics Special Interest Group, and is chair of the BCS Newcastle Branch. He has recently been co-opted onto the Management Board of the Council of Professors and Heads of Computing. Previously he chaired the Learning Development Group for the CPHC and sat on the CPHC management committee.

Jacques Ophoff is a Senior Lecturer in the Department of Information Systems at the University of Cape Town (UCT), South Africa. He obtained his doctorate in Information Technology from the Nelson Mandela Metropolitan University, South Africa. His research interests include behavioral information security, privacy, digital forensics, mobile technologies, and education. He is a regular reviewer for international journals and conferences. He is an active member of the Association of Information Systems and the IFIP WG8.11/WG11.13 Information Systems Security Research group.