Cybersecurity and Cybercrime Combatting Culture for African Police Services

Louise Leenen, Joey Jansen van Vuuren, Anna-Marie Jansen van Vuuren

Cybersecurity and Cybercrime Combatting Culture for African Police Services

Louise Leenen[1] (0000-0002-9212-550X), Joey Jansen van Vuuren[2] (0000-0002-2836-9403) and Anna-Marie Jansen van Vuuren[2] (0000-0001-7923-0447)

[1] University of the Western Cape and CAIR, Cape Town, South Africa
lleenen@uwc.ac.za
[2] Tshwane University of Technology, Pretoria, South Africa
jansenvanvuurenjc@tut.ac.za
Jansenvanvuurena1@tut.ac.za

Abstract. Police forces are responsible to investigate cybercrimes and to protect their own assets from cybersecurity attacks. The majority of police forces find it difficult to fulfil their responsibilities in this regard in the face of constrained funding, a lack of awareness and training amongst law enforcement staff, the growing number of cybercrime incidences, and outdated or insufficient technology and infrastructure.]Even if police forces are able to install technical controls to counter cyber threats, their staff members' cyber behaviour may be a weak link in the cybersecurity chain and will probably not have sufficient training. The cultivation of a cybersecurity culture has been shown to be the best approach to address human behaviour in the cyber domain. There are several frameworks and other resources available for an organisation to cultivate a cybersecurity culture but the organisational culture in law enforcement agencies is different than that in other organisations. The cyber behaviour, cybercrime investigation skills, training and education of police force members require customised strategies and research. African police forces find it particularly difficult to deal with these challenges due to a lack of funding and a shortage of cybersecurity capability and capacity. This paper presents guidelines for African police forces to formulate strategies and plans to train and educate their members and to foster an organisational cybersecurity and cybercrime combatting culture.

Keywords: Law Enforcement, Cybersecurity Culture, Cybercrime Combatting Culture, Police.

1 Introduction

Most organisations have become aware of the risks and threats that accompany connectivity and digitization, and are implementing technical measures and policies to guide employees on ensuring cybersecure environments. One of the most important measures is cybersecurity awareness training. Influencing the cyber behavior of a workforce contributes to the establishment of a cybersecurity culture which will enhance cybersecurity in an organisation [1].

Herskovits [2] defined culture as the collective and shared sense of relatedness of the human experience. There are four categories of culture: macro-cultures, organisational cultures, sub-cultures and micro-cultures [3]. These categories consist mainly of three levels that include espoused beliefs and values, visible artifacts, and basic underlying assumptions.

Cyber professionals refer to the macro-culture in their environment as a "Cyber culture". ENISA (European Union Agency for Network and Information Security) describes Cybersecurity Culture (CSC) as the manifestation of people's behavior with information technologies due to their knowledge, beliefs, perceptions, attitudes, assumptions, norms and values regarding cybersecurity [4]. CSC does not only include cybersecurity awareness and information security frameworks, but is also concerned with making cybersecurity an integral part of an employee's job, habits and conduct. Gcaza, von Solms, & Jansen van Vuuren [5] defined CSC as the aim to "instill a certain way to 'naturally behave' in daily life, a way that subscribes to certain [cybersecurity] assumptions". In addition, a CSC also encapsulates socio-cultural measures that includes technical security methods, to ensure that cyber actions become a natural aspect of the daily activity [6].

People are the weakest link in the cybersecurity chain and are responsible for the majority of data breaches [4,7]. Although various technologies contribute to security, research shows that cybersecurity is mostly influenced by the workforce in companies [6]. It takes time to cultivate a cybersecurity culture but it is crucial to influence and alter the behaviour of users over time to use technology securely [8,9].

This paper applies existing research results on the cultivation of an organisational cybersecurity culture and results on cybersecurity and fighting cybercrime in police forces to propose a framework aimed at cultivating an African Police Cybersecurity and Cybercrime combatting culture (CCCC), which includes the training and educating of police force members to support cybercrime investigations. Section 2 gives an overview of literature on the cultivation of such an organizational culture. Section 3 discusses the structural requirements in a police force for investigating cybercrime, while Section 4 contains guidelines on how to capacitate those structures. In Section 5, the previous sections are combined to produce a step-by-step guide for the cultivation of an appropriate cybersecurity culture in a police force.

2 Cultivation of an Organisational Cybersecurity Culture

Although cybersecurity culture is regarded as an important subject, there are limited published research studies available on the topic [5, 10]. The publications predominantly argue that most important part of such a culture is cybersecurity awareness and education [10,11]. A Norwegian study on their national cybersecurity culture found that businesses coined the term ("CSC") but that not all businesses nor the average citizen were aware of the term [12]. It also noted that Norwegian citizens will willingly accept state monitoring, but do not trust the support from the police when they fall victim to cybercrime.

The Council on Digital Security Risk Management for Economic and Social Prosperity (OECD) recommended the promotion of a cybersecurity culture in order to protect information systems and networks [13]. This culture should include raising awareness of the threats to information systems and networks, as well as the availability of policies, practices, measures and procedures that should be adopted to address those risks. Additionally, law enforcement agencies must promote co-operation and information sharing, and focus on ethical issues in the development of standards. The Council's guidelines for cybersecurity culture development include:

- Raising awareness of processes that could reduce the internal and external cybersecurity risks to information systems and networks, including the potential threats arising from interconnectivity and interdependency.
- Developers, designers and suppliers of products and services must distribute appropriate information about the security functionality of products and services and their responsibilities related to security.
- Ethical conduct is crucial and security consistent with democratic values should be implemented.
- Risk assessment should be conducted to identify threats and vulnerabilities to guide the appropriate selection of controls for cybersecurity risk management.
- Security design and management should be based on risk assessment incorporating all products, services, systems and networks.

ENISA's guide for the promotion of Cybersecurity Culture programs within organisations includes a comprehensive CSC program with best practices. It recognises that organisational behavior is based on shared beliefs, values and actions amongst employees, including the employees' attitude towards cybersecurity. Unfortunately, cybersecurity awareness campaigns have proved to be insufficient. Thus, technical cybersecurity measures must be incorporated with other corporate processes and coexist with job performance. [4]

The main recommendations of the ENISA guide are related to cyber threat awareness within a company. Motivations on why a CSC is needed must be presented to company management and can include threat statistics, evidence of internal cyberattacks and associated costs and results of a either a pilot CSC intervention or successfully deployed CSC programs.

ENISA's CSC Implementation Framework prescribes the following steps:

- Choose a core group of senior staff from different departments. Provision must be made for resources to support the CSC program.
- Conduct a risk assessment of possible misalignments within the organisational culture and business processes.
- Engage employees to get their buy-in.
- Define the main goals of the programme. Some goals will be organisation-wide while others will only be relevant to a certain group.
- Determine the current cybersecurity status and do a gap analysis with the aimed situation.

- Execute activities.
- After the activities have been executed, results must be analysed and measured according to the cybersecurity status.
- A CSC program is a continuous process that needs constant revision.

CISCO's chief information security officer, Steve Martino, emphasised that employees should understand that they are crucial in protecting the company from cybersecurity threats. Martino advised to educate, test and hold employees accountable for cybersecurity without publicly shaming them, but to provide guidance on addressing problems [14]. Still, creating a metric to gauge the level of maturity of a cybersecurity culture, (national or organisational) is challenging [12].

3 Cybercrime Investigation Skills

This section considers the structures required for a police force to investigate cybercrime.

3.1 Cybersecurity and Cybercrime Combatting Skills Shortage

Although there are several dedicated training facilities providing cybercrime training for police forces in the US and in Europe, there is still a skills shortage of cybercrime investigators. A UK government report [15] stated that none of the police forces or regional organised crime units had cybercrime analysts dedicated to developing the understanding of cyber-dependent crime or to support specific cyber-dependent investigations. In addition, if such support was requested from other units it was not prioritised. Trevor Halstead of Cybrary sums up the critical situation: "We really screwed things up this time. Somehow, we are in a situation where the sector of technology with the greatest potential negative impact on our lives, businesses, governments, peace, safety and security happens to have a severe deficiency of qualified people to fill its jobs," [16]. The majority of cybersecurity job positions require a bachelor's degree or higher [17]. Most companies, according to a report of Intel Security in partnership with McAfee, indicated that they prefer at least a bachelor's degree in a relevant technical area to enter the cybersecurity field [18]. The Cybersecurity Skills Gap Analysis (CSGA) report, prepared by the Workforce Intelligence Network for South Michigan, indicates that the highest demand in the US are for cybersecurity analyst/specialists, cybersecurity engineer, auditors, network engineers/architects, and software developers [17,19]. These high-value skills are in critically short supply [18].

The high demand for cybersecurity skills influences the availability of these skills for cybercrime officers in the police. Police forces also need skills on these higher levels to be able to do cybercrime investigations, cybercrime analysis and research. In the case of financial cybercrimes, it is also a requirement to have sufficient knowledge in finance. According to research conducted in Europe by one of the authors, some of the European police forces employ graduates but they rarely have the

skills to do the high-level analytics necessary for cybercrime investigations. An African police force member with these advanced cybercrime skills is an exception. This is confirmed by analysis done by the e-Governance Academy in Estonia portrayed in the National Cyber Security Index (NCSI) for these countries [20]. Non-police force personnel are often used to support cybercrime investigation activities.

3.2 Cybercrime Combatting Positions in the Police

Cybercrime skills requirements vary for different police force positions. One of the authors conducted interviews with members of several police cybercrime units and the results were used to develop the skills requirements for an African police force. Figure 1 reflects a generic framework of the different job levels and skills necessary to combat cybercrime for the police.

These levels differentiate between the cybercrime skills necessary for the general police officer in the local police station; general investigators (the lowest level); cy-

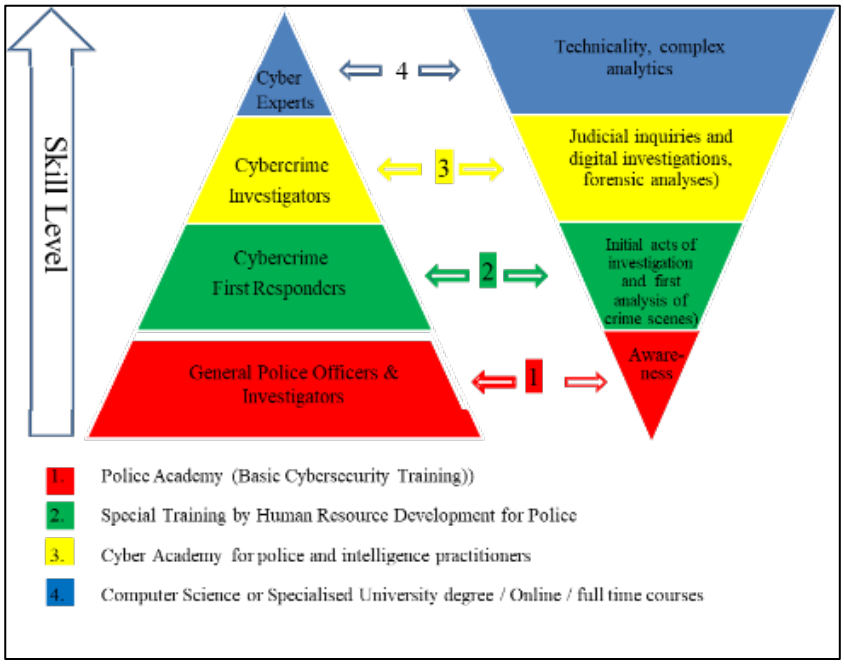

Fig. 1. Cybersecurity Job Levels and Required Skill for the Police.

bercrime first responders responsible to attend to a cyber-crime scene; cybercrime investigators that focus on the investigation of cybercrimes and the cybercrime experts responsible for the analytics, research and predictions of cybercrime. Most of the police cybercrime units will distinguish between the cybercrime investigators and the cybercrime experts. The next section addresses how to acquire these necessary skills and structures.

4 Cybersecurity and Cybercrime Combatting Capability and Capacity Building (CCCC)

The capacity and capability of the police force need to be enhanced to deal with all the technical aspects of cybercrime such as the examination of the digital evidence, the analysis of cybercrime scenes and forensic analysis [21]. Capacity building on different levels of the police force must be part of the cybercrime strategy and it must respond to the needs of police officers. It further produces immediate impact, favours multi-stakeholder cooperation and contributes to human development [21]. In addition, all cybercrime investigators will have to deal with electronic evidence and need comprehensive training in this regard [22].

Police officers have different training needs according to the required skills for their position. These job skills normally include generic investigation; cybercrime first responder and cybercrime scene investigation; internet crime investigation; covert internet crime investigation; network crime investigation; and digital forensic investigation and management) [23]. They can be categorised in four levels (Fig. 1):

- The general policeman in a local police station needs generic cybersecurity awareness training and cybercrime reporting skills.
- The cybercrime first responder needs the competency to secure electronic evidence and carry out computer forensics analyses for criminal proceedings.
- The cybercrime investigator needs to be able to conduct cybercrime, internet crime, covert internet crime, network crime, and digital forensic investigations and analyses.
- The cybercrime expert needs to be able to do advanced cybercrime analytics.

Different methodologies and platforms can be used to do the training. The UK Law enforcement agencies and partners make use of an online learning facility. In 2018, they established a specific area called the Cybercrime Hub intended to be “a one stop shop for all officers and staff with an interest in cybercrime, that will train from officers little knowledge to experienced cyber investigators” [15].

General Cybersecurity Awareness Training

Awareness training can be done online using different platforms, e.g. a virtual reality training program on mobile devices in the form of games. The establishment of a cyber academy responsible for cybercrime training in different African regions is recommended.

The functions of police officers will determine the appropriate level of training which must be scalable, standardised and replicable. It is possible to adapt existing police force training materials and initiatives [22] to include cybersecurity, cybercrime reporting and investigation procedures. There must also be cooperation between law enforcement, academia and industry. To ensure sustainability it is important to include the training of trainers.

First Responder Training

The goal of first responder training according to the FBI's special agent James McDonald, "is to improve a first responder's technical knowledge by focusing on best practices in terms of investigative methods specific for cyber investigations." He also emphasised that if first responders are trained there are less chance of errors being made while securing a crime scene involving digital evidence [24]. They need to have a working knowledge on how to secure electronic evidence as well as the physical evidence, while documenting the crime scene, and have knowledge of software, hardware, the Internet, social networks, encryption, legal tools, and other digital evidence. They also need enhanced practical skills regarding the methodology used in digital forensics for identifying and responding effectively at the scene of cybercrime cases [25].

Cybercrime Investigator Training

In addition to the normal investigator training, cybercrime investigator training has to include knowledge on digital media, networks and databases, operating systems, the use of forensic tools and the ability to do technical legal analysis of evidence, metadata, backup systems, electronic storage, applications, mobile and internet communication, the cloud and specific digital devices. They need to understand the attitudes required for cybercrime investigation, including the systematic management of cybercrime investigative resources and staff [26]. Some of the basic training can be done online. Practical training, e.g. forensics, must be done with the correct equipment in laboratories. A cybercrime investigation manual and discussion groups can support and guide cybercrime investigations [15]. A Cyber Academy for the training of intelligence officers and cybercrime investigators can also be established.

Cybercrime Experts

Tertiary degrees need to be developed where students can incorporate knowledge from criminology and computer science; they need to develop critical thinking and investigative skills, sophisticated technological understanding and advanced technical computer science skills. Studies must include advanced networking, databases, software and operating systems skills as well as all the platforms used to protect systems e.g. firewalls and intrusion detection systems. It must also include guidance on how cyber criminals could extract financial data, exploit children through social networking or destruct process control systems, and an ethical hacking course.

5 Cultivating a Cybersecurity Culture in a Police Force

In this section, we present a framework (Table 1) for establishing and running a Cybersecurity and Cybercrime Combatting Culture (CCCC) program in a police force as adapted from prior research [27]. Each phase is expanded below the table.

Table 1. A framework for a Police Officer CCCC program

Preparation Phase	Design Phase	Execution Phase
a: Cybersecurity and cybercrime strategies and policies must be in place.	**1**: Set up the core CCCC task team.	***i***: Run awareness and educational campaigns.
b: All police officers must be included in the program.	**2:** Define main goals, success criteria and target groups.	***ii***: Implement training programs online and run competitions to ensure cybercrime awareness. Run cybersecurity exercises.
c: Understand current culture and processes, and access the risks.	**3**: Identify roles and responsibilities and develop training material.	***iii***: Measure the success of training exercises
d: Set up an initial baseline, i.e. the current behaviours.	**4**: Identify supporting divisions.	***iv***: Return to Step 6
e: Run a pilot activity and measure its impact.	**5**: Design cybersecurity and cybercrime exercises and competitions with identified metrics.	
f: Get buy-in from upper level command.	**6:** Review and update the program.	

5.1 Preparation Phase

Step a: Setting up Cybersecurity and cybercrime strategies and policies

The CSC program aims to foster a culture where cybersecurity and cybercrime policies and knowledge become instilled in members of a police force. It supports the cybersecurity governance and best practices prescribed by the cybersecurity strategy and policies, including ethical conduct and values. Support for this program must come from all role players including IT support services and cybercrime investigators. The cybersecurity policies must include a description of the distribution of appropriate information, including updates, in a timely manner to enhance police officers' understanding. It must include a Cybersecurity Risk Management Program that includes risk assessment, the monitoring of networks to prevent and detect incidences, measures on the response to incidents as well as systems recovery and maintenance. These policies must be implemented in such a way to create an integrated, coherent system of security to protect the police's own systems against cyber criminals.

Step b: All police officers be included

All police officers must be trained according to the capability and capacity building program (Section 4), and included in the CCCC program. The IT staff that maintains the police network and systems must also be trained and certified to protect their own systems.

Step c: Understand current culture and processes, and access the risks

The CCCC program staff must engage with police force members to determine the existing cultures in the police force units and divisions. Risk assessment should be conducted to identify current threats and vulnerabilities. This will identify misalignments between existing practices and processes and security measures which may require engagements to find resolutions that will ensure commitment from all.

Step d: Set up an initial baseline

Determine the current maturity level of the current CCCC by using appropriate metrics. Some metrics are published by the Payment Cards Industry [28]. This can be refined and used for the measurement of the impact of the program.

Step e: Run a pilot CCCC activity and measure the impact

Run a small pilot program within a single unit. On completion of the pilot, changes in the selected behaviour against the baseline can illustrate the potential impact. For example, the activity of using a password storage app instead of storing personal passwords in a plain text. It will be easy to measure improvement after this activity.

Step f: Get buy-in from the upper level command

Strong motivations must be developed to convince the commissioning staff to support and fund the CCCC program. These programs require financial and human resources, funding and a dedicated team to run and adapt the program over time. The motivation can be done by incorporating:

- Current cyber threats statistics including global, national and regional data.
- Evidence of cyber-attacks in the police.
- The results from the pilot activity.
- Estimates of the financial and reputational impact of cyber-attacks and breaches.

5.2 Design Phase

Step 1: Set up a core CCCC task team

The core task team is responsible for the development, implementation and maintenance of the CCCC program and must represent a cross-section of the police force by including members of different units. The team must understand the group cultures in the different units. Adaptations of the program can be made for individual groups if necessary. The core group must be continuously supported by the senior commissioning officers to formulate CC policy and strategy and to oversee the implementation and execution of the program. The team must also allow different divisions and units to give inputs and feedback on the implementation in their group to ensure participation in the long run, to make use of their internal expertise, be innovative and feel they contributed.

Step 2: Define main goals, success criteria and target groups

Define the main goals for the CCCC program that prioritise the most important issues and criteria for the target group's successes. The impact of adversary cyber exploitation must be kept at an acceptable level according to standardised processes for assessing risk to mission assurance [29], and every member has a role and a responsibility to achieve this.

Criteria of success measurements must be identified in an early stage. Performance outcomes are critical and it is important to measure the actual state of cybersecurity and the impact of the program. More complex measurements will also be needed because culture consist of more than only behaviours; it also includes values, attitudes and perceptions about cybersecurity. Mlamedal & Roislien [12] motivate the identification of a robust set of indicators that enable the creation of an appropriate baseline for the measurement of a CCCC. Accountability by members are also important [29].

Threat exchange of cybersecurity information must be distributed on a regular basis to police officers.

The identification of target groups is complex due to each division having its own organisational culture. A CCCC will not be successful if it is enforced on a group; it must be cultivated over time, with the required adaptations. Examples of different target groups are the Senior Management: Commissioned Officers, Commissioning Officers, Non-Commissioning officers, IT providers and the Cybercrime units.

Step 3: Identify responsibilities of task members and develop training material

Responsibilities are assigned to IT support police officers according to the risk assessments. These assessments include risks due to system vulnerabilities, threats to systems and the impact to a police officer's missions. All security controls for programs must be supplemented with cybersecurity measures. Training materials must be developed according to the job profiles.

Figure 2 depicting the roles is an adaptation from a figure in that appeared in [27].

Step 4: Identify supporting divisions

Support for the initiative must come from all the service departments in the police force. Commissioning officers at every level should actively be encouraged to participate in the program by including performance in the program into performance reviews.

Step 5: Design cybersecurity and cybercrime exercises and competitions with identified metrics

Cybersecurity and cybercrime assessment exercises can be developed to evaluate the preparedness of all police units. These exercises are an effective way to measure the level of collaboration and information sharing between the different divisions and units. They must cater for different target groups. Different platforms such as videos, instructor-led training, quizzes, games, email, internal social media etc. can be used. In addition, cybersecurity drills can be arranged for units [21]. Communication is important to

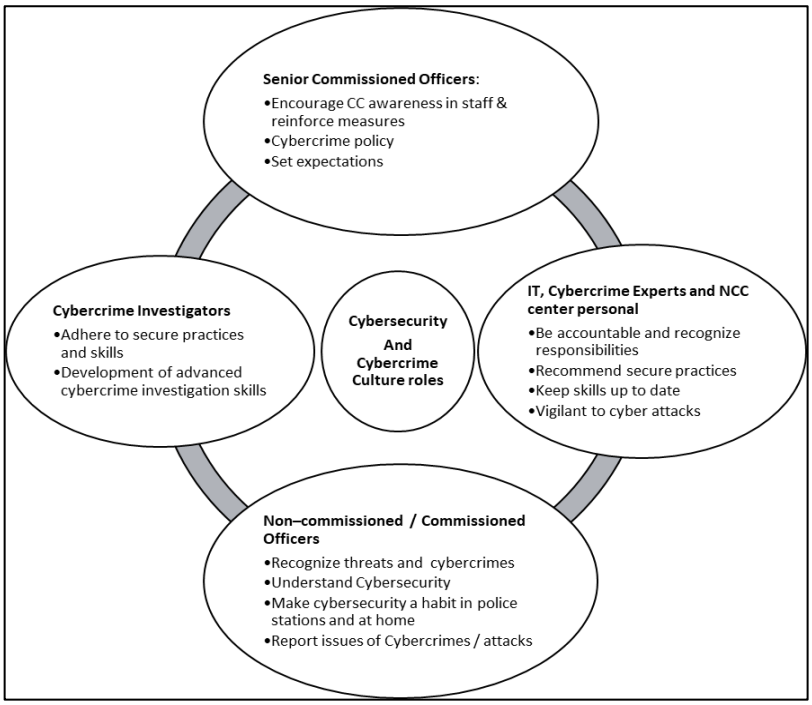

Fig. 2. Cybersecurity and Cybercrime Combatting Culture Roles for the Police Force

emphasise the necessity of the exercises and to ensure continued participation. Exercises must also include the identification of cybercrimes and the assessment of correct measures taken in the evaluation of a cybercrime scene. A set of metrics must be established to measure success.

There also must be customised exercises for senior commissioning officers focused on policies. These activities must include activities geared for staff with knowledge levels ranging from no technical knowledge to a high level of IT knowledge and competence. A Best Practice manual must accompany all training material to encourage the adoption of practices aimed at promoting secure online behaviour.

Step 6: Review and update the program

Culture is dynamic and the CCCC program has to be updated frequently. CCCC should become part of the Police Academy training and HR Development programs. The Cybersecurity Risk Management Program must be used to reassess the status of cybersecurity on a regular basis to make provision for new and changing threats and vulnerabilities, and to adapt security policies, practices and procedures. Measurements and the baseline must be updated to make provision for the changes.

5.3 Execution Phase

Step i: Run Awareness and Educational Campaigns

Education and awareness for force members are essential elements of a cybersecurity culture. The emphasis must not only be on technical, administrative and procedural measures to protect computer systems, but also to keep member informed on the latest threats through awareness campaigns. In addition, due to the national cybercrime centres' research and 24/7 centres' international co-operations, these types of centres can be the key points of contact for cybersecurity matters and can facilitate information and technology sharing for the creation of awareness in the police force.

Step ii: Run Cybersecurity Exercises

The focus of these exercises is to evaluate the preparedness of staff in police units as well as to support structures to deal with cyber-attacks. Cybersecurity drills are also an option. The most effective exercises for senior commissioning officers are scenario-based. Cybersecurity experts must facilitate these exercises that can include, among other things, the loss of connectivity that interrupts the communication, and ransomware exercises. Special weeks can be identified for the hosting of exercises e.g. during Cyber Security Month (usually in October) that can be aimed at reaching a large number of police officers.

Step iii: Measure the success of the exercises

Several metrics can be used to measure performance [28]. For example, if an activity's aim was to make participants aware of the importance of logging out of workstations when they leave an office, the baseline will be the number of workstations that were open in the absence of the user (physical inspection) before the activity. The current behaviour can be determined by a similar count after the activity was run.

Step iv: Return to Step 6

This programme for cultivating a CCCC in a police force needs to take place once the necessary structures are in place (Section 3), and needs to run in conjunction with ongoing capacity and capability building (Section 4).

6 Conclusion

Cybersecurity awareness and appropriate cyber behaviour in a police force is often neglected even when police offers receive training to combat cybercrime. The cultivation of a cybersecurity culture in a police force is essential to protect their systems and to support other cybersecurity training. Although there are several frameworks and other resources available for an organisation to cultivate a cybersecurity culture, law enforcement agencies face a different environment. This paper considers frameworks and resources on the cultivation of organisational cyber-

security culture to present a customized framework for a police force. In addition, requirements to create a cybercrime combatting culture in a police force environment are specified. The paper thus presents comprehensive guidelines in this regard that can be implemented and applied by police forces in Africa.

References

1. Newhouse W, Keith S, Scribner, B, Witte G (2017) National initiative for cybersecurity education (NICE): Cybersecurity framework. NIST Special Publication 800-181. doi:10.6028/NIST.SP.800-181
2. Herskovits MJ (1948) The contribution of Afro-american studies to Africanist research. American Anthropologist, vol 50(1). pp. 1-10. doi:10.1525/aa.1948.50.1.02a00020
3. Schein EH (1985) Organizational culture and leadership. A dynamic view. Jossey-Bass, San Francisco. doi:10.1002/hrm.3930240312
4. European Agency for Network and Information Security (ENISA) (2017) Cyber security culture in organisations. doi:10.2824/10543
5. Gcaza N, Von Solms R, Jansen van Vuuren J (2015) An ontology for a national cybersecurity culture environment. In: The nineth international symposium on human aspects of information security and assurance (HAISA). pp. 1-10
6. Reid R, van Niekerk J (2014) Towards an education campaign for forstering a societal cyber secure culture. In: The eighth international symposium in human aspects of information security and assurance (HAISA). pp 174-184.
7. Ponemon Institute (2017) The human factor in data protection. https://www.ponemon.org/blog/the-human-factor-in-data-protection
8. Gcaza N, van Solms R (2017) Cybersecurity culture: An ill-defined problem. In: IFIP World Conference on Information Security Education (WISE), pp. 98-109.
9. Schlienger T, Teufel S (2003) Information security culture - from analysis to change. South African Computer Journal, Vol 31, pp 46-52.
10. International Telecommunications Union (2008) ITU Corporate Annual Report. https://www.itu.int/osg/csd/stratplan/AR2008_web.pdf.
11. Kortjan N, Von Solms R (2012) Fostering a cyber security culture: a case of South Africa. In ZA-WWW, 2012 Conference
12. Mlamedal B, Roislien HE (2016) The Norwegian cyber security culture. Norwegian Centre for Information Security (NorSIS). https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf
13. OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. (2015) https://legalinstruments.oecd.org/en/instruments/116. OECD/LEGAL/0415.
14. Veltsos C (2017) Building a cybersecurity culture around Layer 8. Security Intelligence. https://securityintelligence.com/building-a-cybersecurity-culture-around-layer-8/

15. HMICFRS (2019) Cyber: Keep the light on. An inspection of the police response to cyber-dependent crime. https://www.justiceinspectorates.gov.uk/hmicfrs/publications/keep-the-light-on-police-response-to-cyber-dependent-crime/
16. Florentine S (2015) Closing the cybersecurity talent gap, one woman at a time. https://www.cio.com/article/3005637/cyber-attacks-espionage/closing-the-cybersecurity-talent-gap-one-woman-at-a-time.html.
17. Workforce Intelligence Network for Southeast Michigan (2017) Cybersecurity skills gap analysis. https://winintelligence.org/wp-content/uploads/2017/07/FINAL-Cybersecurity-Skills-Gap-2017-Web-1.pdf.
18. CSIS Intel Security (2016) Hacking the Skills Shortage. https://www.csis.org/programs/technology-policy-program/cybersecurity-and-warfare/other-projects-cybersecurity-0.
19. NICE Cybersecurity Workforce Framework Work Roles (2017) National Initiative for Cybersecurity Careers and Studies. https://niccs.us-cert.gov/nice-cybersecurity-workforce-framework-work-roles.
20. e-Governance Academy (EGA) (2018) National Cyber Security Index 2017 South Africa. https://ncsi.ega.ee/country/za/
21. Usmani KA, Appayya JA (2017) Capacity building is the key to fight against cybercrime: The Mauritian perspective. Global Cyber Expertise Magazine, vol 4.
22. Global Project on Cybercrime (2013) Capacity building on cybercrime. http://www.combattingcybercrime.org/files/virtual-library/capacity-building/capacity-building-on-cybercrime.pdf.
23. Seger A (2012) Cybercrime strategies. Global Project on Cybercrime. https://rm.coe.int/16802fa3e1
24. Federal Buro of Investigation (FBI) (2016), Offer online cyber training for law enforcement first responders. https://www.fbi.gov/news/stories/online-cyber-training-for-law-enforcement-first-responders.
25. Christopoulos G (2017) First responders and cyber forensics. https://www.cepol.europa.eu/media/blog/first-responders-cyber-forensics.
26. Shook S (2019) Cybercrime investigation body of knowledge. https://www.cibok.org/en/.
27. Leenen L, Jansen van Vuuren JC (2019) Framework for the cultivation of a military cybersecurity culture. In: 14th International Conference on Cyber Warfare and Security (ICCWS)
28. PCI Security Standards Council (2014) Best Practices for Implementing a Security Awareness Program. https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.
29. Snyder D, Powers JD, Bodine-Baron W, Fox B, Kendrick L, Powell MH (2015) Improving the cybersecurity of U.S. Air Force military systems throughout their life cycles. RAND Corporation