Cybersecurity as a response to combating Cybercrime: A Contextual appraisal of the African region

Mphatheni Mandlenkosi Richard

Key concepts

- Computer
- Cybercrime
- Cybersecurity
- Internet




Introduction

- Cybercrime includes all illegal acts committed through electronic use. It requires electronic operations aimed at cracking the security of a computer system and compromising the data processed by the computer (Malby, Mace, Holterhof, Brown, Kascherus & Ignatuschtschenko, 2013).

Cybercrime and cybercriminals

- Cybercrime may results in illegal activities resulting in pecuniary losses while others include violent crimes against individuals or their property such as identity theft and blackmail.
- Similar to traditional crimes, the commission of cybercrime relies on the crime triangle (Cross & Shinder, 2008), which constitutes three factors: a victim, a motive, and an opportunity.
- The victim is the intended and/or actual victim of an attack (physically or digitally), motive is what motivates the criminal to carry out the attack, and opportunity is what makes the commission of the intended crime possible

The nature and extent of cybercrime and cybersecurity in Africa

- Cybercrime does not only affect governments and organisations, but individuals as well.
- According to estimates by Microsoft (2014), about half of all adults who use the Internet have been cybercrime victims.
- With reference to data provided by a British consulting firm, Kshetri (2019) estimates that about a billion people in Africa will have access to the Internet by 2022.
- The projected billions of people in Africa with Internet access will not all be law-abiding citizens and that a significant number of these people will be opportunistic criminals

The nature and extent of cybercrime and cybersecurity in Africa

- African countries with fast-growing economies are well advised to be ready to protect critical documents, vulnerable digital systems, as well as industries and businesses from cyber threats (Peter, 2017).
- Institutions with financial resources are already investing heavily in cybersecurity to safeguard their resources but, if cyberattacks are on the increase, these vast amounts of money will have been spent in vain.
- In South Africa, many institutions, particularly those with significant financial capacity, are at high risk of cyberattacks (South Africa, 2020)

Securing the cyberspace

The following measures are recommended for safety in the cyberspace:

- Individuals need to play a critical role as frontline users of the Internet in the fight against cyberspace crime;
- Individuals, organisations, and governments must frequently install anti-virus programmes, scour for viruses, and keep fire walls updated;
- Individuals must be critical of what they put online and which websites they enter

Cyber security in Africa

South African citizens and business operators must become more resilient in their efforts to defend their operations and/or safeguard their customers.

According to Mcanyana and Brindley (2020), iDefense suggests several measures to curb cybercrime such as improving security intelligence; devising protection against internal threats and people-based attacks; and focusing on compliance (Mcanyana & Brindley, 2020: 10).

Challenges in addressing cybercrime

- The ever-emerging new features that occur in cyberspace create ever-evolving opportunities for digital crimes

✔ *Globalisation*

✔ *Distribution*

✔ *Synoptics and panopticism*

✔ *Data trails*

Summary

Prevention measures aimed at combating cybercrime are insufficient due to a lack of a universal definition of cybercrime. As a result, international organisations and the global community must reach an agreement on what constitutes cybercrime.

A shared understanding of what constitutes cybercrime will aid in the effective prosecution of cybercrime. Combating cybercrime and ensuring Cybersecurity necessitate global collaboration. Organisations and businesses should have departments/units dedicated to dealing with cybercrime and cybersecurity breaches.

Personnel with advanced knowledge of cyberspace must be assigned to such a unit or department. Personnel with extensive knowledge of cyberspace will deduce cybercriminals' motivations and assist in apprehending the criminals and devising new measures to prevent future cyberspace breaches.

Summary

An integrated and collaborative approach should be adopted to ensure that all relevant stakeholders in the public and private domains work together to devise and implement workable safety and security policies. However, as policies are notorious poorly implemented and policed, practical implementation strategies need to be devised as a matter of urgency.

Thank You

Mandlenkosi Richard Mphatheni

Mandlenkosi.mphatheni@ul.ac.za

University of Limpopo