Five things South Africa must do to combat cybercrime

September 6 2022, by Basie von Solms

Credit: AI-generated image (disclaimer)

Cyber-attacks are on the rise globally, with seriously negative implications for countries' strategic, national, economic and social well-being.

A cyber-attack can be defined as an unauthorized attempt—successful or

not—to infiltrate a computer or computer system for malicious purposes. Reasons for such attacks vary from financial gain to espionage, gathering strategic and national information and intelligence about an adversary. Such an adversary can be a nation state, a corporate entity or a private individual.

The authoritative international Cybercrime Magazine expects global cybercrime costs to grow by 15% a year over the next five years, reaching $10.5 trillion a year by 2025, reporting: "This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined."

A 2022 report by Surfshark, the Netherlands-based virtual private network (VPN) service company, lists the top 10 countries in the world in terms of cybercrime density. Cybercrime density is defined as the percentage of cyber victims per one million internet users. South Africa is number six on the list, with the U.K., the U.S., Canada, Australia and Greece taking places one to five. The U.K., therefore, has the highest cybercrime density. That means it has the most cybercrime. One reason for South Africa's poor showing may lie in the fact that a 2020 Accenture report found the country's internet users were inexperienced and less technically alert.

In May, a data leak at Transunion, a credit management company, reportedly compromised the personal information of 54 million South Africans. President Cyril Ramaphosa was among the victims.

In 2021 a successful cyber-attack on Transnet, the transport parastatal, brought container terminals to a standstill, disrupting imports and exports. This had massive strategic and economic implications.

Cybercriminals are increasingly moving from targeting enterprise systems to the end users—the employees who operate computers and have access to the enterprises' corporate data and network systems.

Poor cybersecurity awareness and training of end users is one reason cyber-attacks succeed in South Africa. In both the Transunion and Transnet attacks, unauthorized access was gained via end users.

Cyber-attacks are expected to grow in sophistication as criminals exploit such technologies as artificial intelligence. I am a cybersecurity expert and academic who has watched the growing problem of cyber-attacks in South Africa and internationally over the last 30 years. In my experience, five key ingredients need to be in place in the cybersecurity ecosystem to fight cybercrime in South Africa:

- recognition of cybercrime as a governance issue
- skilled practitioners and advisors
- savvy citizens
- public-private partnership
- a dedicated "national director of cybersecurity."

The five key ingredients

1. Fighting cybercrimes must be a governance issue

This is a core principle in all national and international good corporate governance practices. In private companies that role falls on the boards of directors and executive management. It's part of the oversight and code of conduct of top management.

For the government it means that the president and cabinet should be responsible for ensuring that the country is resilient against cyber-attacks.

2. Skilled cyber practitioners and advisors are vital

There is a dire need for cybersecurity capacity globally. South Africa is no exception.

This shortage is experienced both in government and in the private sector. South Africa needs a large number of cybersecurity practitioners and advisers to help users to identify and prevent cyber-attacks. These should ideally be available in all government institutions, including every municipality, hospital and school.

The skills shortage is being addressed by universities and private colleges, but this is but a drop in the ocean because the output is limited and takes several years to produce. The fact is that such cybersecurity practitioners do not necessarily all have to have university degrees. In the U.K., for example, the government's National Cybersecurity Center has a program called CyberFirst, directed towards schools.

Such a program could have significant benefits for South Africa, including providing jobs for talented young people who do not have the money or interest to pursue tertiary studies.

3. Citizens must be cybercrime savvy

All computer end users must be empowered to be cybercrime fighters to make the country, companies and other institutions more resilient.

Security is everyone's job. Everyone from the entry-level to top management should know how to identify and report breaches so they can defend the enterprise.

New, more effective approaches must be found to make end users more

aware of cyber risks and integrate them better into the enterprise's cyber defenses. One example of such a new approach can be modeled on the idea of a human firewall, where every end user understands that he or she is part of the cyber defense of the country or company, and acts in that way.

4. Public-private partnership is imperative

The government cannot fight cybercapture on its own. Most of the present cyber expertise lies in the private sector. The private sector is basically running a major part of South Africa's critical information infrastructures—such as for banks, internet service providers and cellphone service companies.

Public-private partnerships must be established as soon as possible to combat cybercrimes. This idea is already provided for in the original National Cybersecurity Policy Framework of 2013. But the political will from government to make it work seems missing and no such partnerships have really developed.

5. Have a dedicated 'national cybersecurity director'

Cybersecurity experts and functionaries in the government and the private sector often operate in independent silos. Nobody has the required "helicopter view" and oversight of the status of cybercrime in the country. Not sharing scarce cybersecurity expertise between role players ends up in expensive duplication of expensive software systems and training, which could be more widely available.

South Africa needs a national bureaucrat, or "national cybersecurity director" to play an oversight role. The office must act as a single point of contact for all cyber-related matters in the country. The incumbent

must be technically skilled in cyber matters, and have the trust of both government and private sector role players.

He or she must report directly to parliament—something like Chapter 9 institutions, which strengthen the country's democracy—as provided under the constitution.The U.S., the U.K. and Rwanda have all created such a position or agency.

Provided by The Conversation

Citation: Five things South Africa must do to combat cybercrime (2022, September 6) retrieved 3 May 2024 from https://techxplore.com/news/2022-09-south-africa-combat-cybercrime.html