Addressing the local cybersecurity skills shortage

By Marcus Karuppan

14 May 2019

The PWC Global Economic Crime and Fraud Survey published in 2018 states that over a quarter of South African respondents believe that cybercrime will be the most disruptive, impactful crime faced over the next two years. This is especially alarming in the face of the continuing shortage of cybersecurity skills plaguing South Africa at a time when we need them most.

Marcus Karuppan

The lack of cybersecurity skills coupled with the rising youth unemployment problem creates the ideal opportunity for South African businesses, education facilities and government to collaborate and fill both gaps. In fact, the ability to develop ICT skills within our borders could make South Africa a choice global provider of ICT and cybersecurity skills – if we address this now.

The in-demand skills

Despite the increase in ICT courses and academies across a range of disciplines, the skills required to operate, support and understand the complexities of next-generation technologies and today's cyber threats are still underdeveloped.

We are living in a world where cybercriminals are smart and are using the latest technologies to infiltrate networks and achieve their goals. To keep up with the threat landscape requires a deeper set of skills and insight into cybersecurity than we currently have enough of. The skills being taught are traditional security controls, typically around protecting the perimeter. This is still relevant, however as businesses digitally transform, moving to the cloud and investing in connected, smart technologies, security becomes far more complex.

A level of data science knowledge, to understand the flow of data across digital platforms, is essential to today's cybersecurity skills pool. Data no longer resides on premise and can be anywhere from various endpoints, to the cloud, to traversing across multiple networks. A deep understanding of where data is, coupled with understanding the threats at every point is necessary to ensure the adequate controls and technologies are put in place to protect it.

It's also vital to be more proactive than preventative, and the ability to quickly detect what is happening to a business' data at any time is critical.

Recruiting for today's requirements

Recruiting to fill a cybersecurity position is increasingly challenging for organisations. Many tertiary ICT programs focus on general computer science, covering the basics of cybersecurity. Experience is vital, yet school leavers lack the experience and businesses are reluctant to hire inexperienced individuals, creating a catch twenty-two situation.

As a country, we need to rethink the ICT education curriculum from as early as primary school, educating learners – who often possess some form of a smart device from as young as ten years old - on cybersecurity and risks for their personal devices. Learners who are working on computers or tablets at school should learn how to protect the devices as well as how to use them, making risk awareness part of their sphere of understanding from a young age. This prepares cybersecurity professionals of the future, giving them a strong foundation to build on.

Training for the future

Beyond this, businesses and tertiary education institutions can be doing a lot more collaboratively to build the local skills pool. Learnerships, bursaries and apprenticeship-type programs for school leavers is one way to ensure that school leavers receive hands-on field experience, preparing them for the realities of the cybersecurity landscape and ensuring they are equipped to deal with today's level of threats.

Often, students who enter the cybersecurity discipline find themselves confronted with limited exposure to cybersecurity. They are often trained purely in one product or technology or exposed only to security policy frameworks. Students need to be given access to broader knowledge, that spans multiple technologies, products, policies and controls. They should also be exposed to the threats that are out there, giving them the ability to identify, understand and, thus, prevent them.

Businesses can also upskill internally, providing training and experience to those already within their organisation who display an affinity for cybersecurity skills. There are a number of online resources that businesses can employ to upskill and train internal employees to fill the gap.

Creating the pool

South Africa is uniquely positioned to be able to become a global cybersecurity resource pool. We have comparatively inexpensive resources, and the cost of importing resources from our shores is not very high for Europe or the States. We also have access to world-class education resources and skills academies. It makes sense to use these resources to develop the skills of our unemployed youth and become the cybersecurity resource pool of choice, reducing unemployment, filling the skills gap and also making for a safer local cyber landscape all at once.

ABOUT THE AUTHOR

Marcus Karuppan is ICT Academy Manager at T-Systems South Africa