We need to up our game in the fight against cybercrime, and quickly

By Jason Jordaan

22 Sep 2015

Governments will have to invest in the fight against cybercrime if we are to mitigate the increasing risks brought on by the Internet of Things (IoT). If our South African law enforcement is to stand any chance in winning the battle against these highly skilled criminals, they will have to invest in hiring people with high-tech skills. This is the view of Jason Jordaan, principal forensic scientist at DFIRLABS.

©Engin Korkmaz via 123RF

"While a lot of work has been done towards a new cybercrime and cybersecurity bill for South Africa, we do not only need policies that address cybercrime robustly and openly, but also highly skilled law enforcement officials. The challenge is that these skills come at a very high price," he says. "We also need to see a lot more collaboration in the battle against cybercrime. Civil society, for example, needs to take an active role in educating citizens on what cybercrime is, what the risks are and how to identify potential cyberattacks."

Cybersecurity is one of the key areas that will be addressed by this year's MyWorld of Tomorrow conference and exhibition. Aimed at driving African innovation to solve African challenges, MyWorld of Tomorrow will showcase great ideas, products and solutions, while bringing together great minds to innovate for the future.

More collaboration is needed

Jordaan adds that there is a false sense of security within organisations, which means they have a tendency to invest security technology rather than security professionals. "There is a lot of technology out there that address certain threats, but we have to realise that cybercrime is driven by highly skilled humans. The best way to prevent these threats and catch cybercriminals is through people who have the right skills to do so. Companies need to invest more in their security and ensure they have well-equipped security departments."

He adds that organisations often think that the state will resolve cybercrime issues for them, but that is not realistic. "When organisations get hacked, they call the police, believing this will sort out the issue. Even government and law enforcement is struggling with this. Already we don't have the capacity to deal with normal crime, let alone cybercrime. Organisations need to take ownership of the risks and collaborate more to find a way to mitigate these risks."

We are not taking it seriously enough

According to Jordaan, cybercrime is often perceived as a nuisance crime and not taken seriously enough. "We need to understand that cybercrime is this absolutely pervasive crime and every single person who has access to the internet is a potential victim. It's also very serious, because it's so easy to commit, yet so difficult to catch the perpetrators. IoT is going to make this ten times worse and make it ten times harder to bring the criminals to book."

IoT, in a nutshell, refers to everything connecting to everything with the internet being the common thread and Jordaan believes that we have only hit the tip of the iceberg. "We haven't quite reached an environment where IoT is a complete reality, so at this stage the threats are hypothetical. The moment we start to see IoT become real, more threats will emerge." He adds that with more connected devices, hackers could for example gain access to your IP cameras, using your own security systems to spy on you.

"Any crime we can think of today, will be made easier by IoT. Take hospitals for example. In a 'connected' hospital each drip has an RFID tag. If I want to target someone in that hospital, I could hack into the hospital's system, alter the RFID tags of the medication prescribed to the person I want to harm and could do them serious physical harm or even commit murder by 'prescribing' harmful substances to them. Nobody is going to question the system, paving the way for disastrous consequences."

From virtual to physical

"The fact that cybercrime can move out of the virtual into the physical world as a result of IoT can see these crimes causing real harm to people and property and if we are not ready for it, it will hit us hard. You can no longer just focus on protecting corporate and citizen data alone - when non-traditional devices become connected it opens up a whole new world of risks," says Jordaan. "At the end of the day we need to see government, civil society and corporate South Africa stand together in this fight. You will never be able to prevent all crime, but as a collective we can definitely manage it and mitigate some of the risks," he concludes.

ABOUT THE AUTHOR

Jason Jordaan, principal forensic scientist at DFIRLABS