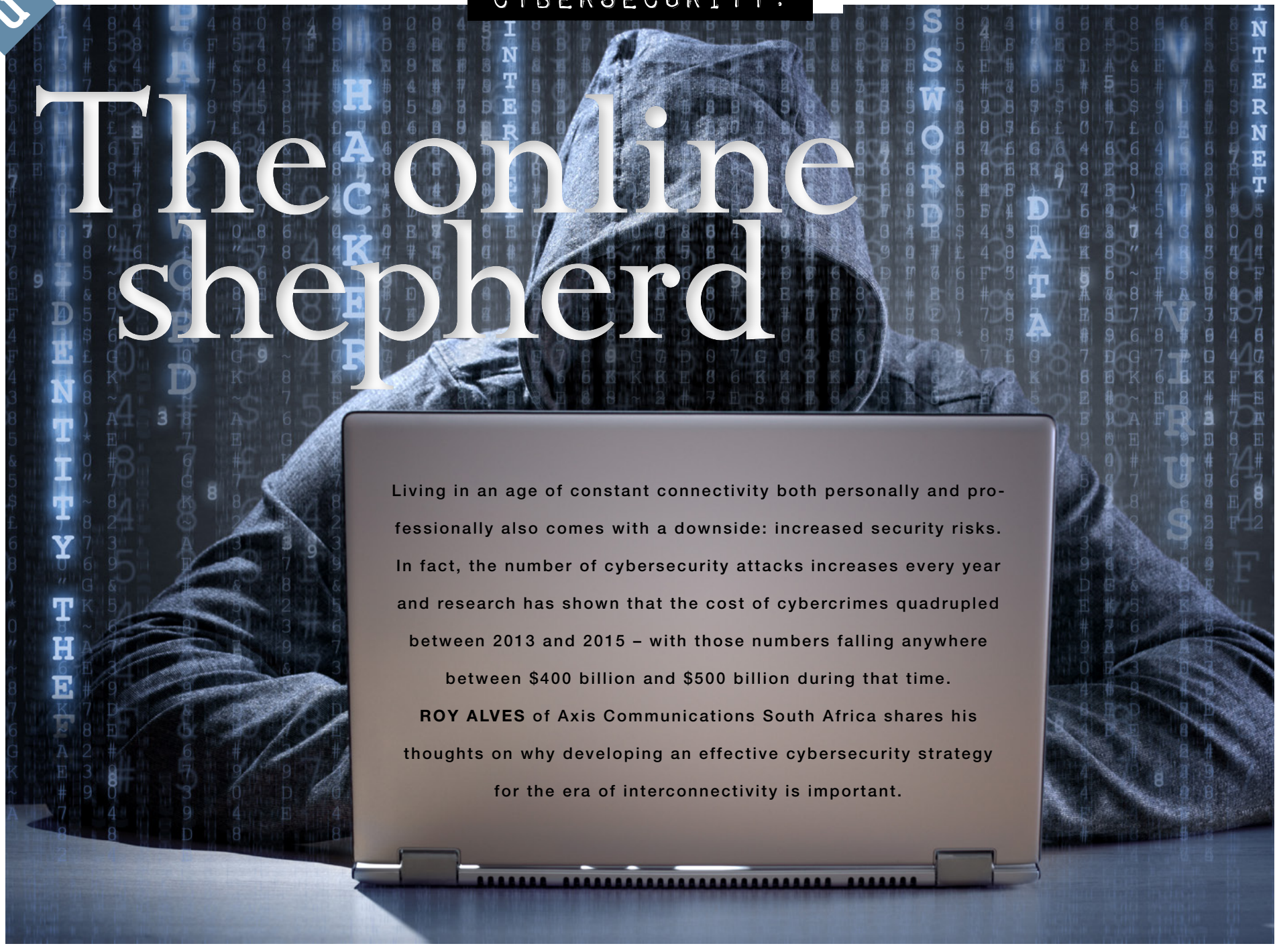
The online shepherd



Living in an age of constant connectivity both personally and professionally also comes with a downside: increased security risks. In fact, the number of cybersecurity attacks increases every year and research has shown that the cost of cybercrimes quadrupled between 2013 and 2015 – with those numbers falling anywhere between $400 billion and $500 billion during that time.

ROY ALVES of Axis Communications South Africa shares his thoughts on why developing an effective cybersecurity strategy for the era of interconnectivity is important.

Within the modern business environment, employees can communicate and collaborate with customers and colleagues from anywhere and anytime, using virtually any device or platform because of technology trends such as mobility and cloud computing. In this era of interconnectivity, information can also frequently flow between the business and suppliers or partners, while employees utilise big data analytics solutions to gather and disseminate an ever-increasing amount of data on consumers and market trends as well opportunities. While the interconnectivity has led to efficiency gains on an individual and company-wide level, it has also led to increased security risk, because it has made cybersecurity and physical security more complex.

To mitigate risks in this kind of an open ecosystem, you need all the vendors operating off the same cybersecurity playbook.

Where a security manager in charge of physical security systems might have exclusively focussed on creating a closed system that can never be breached, s/he must now adopt a more ecosystem-centric approach. This is the result of converging technologies, with the industry migrating from analogue to IP-based technology for instance, and making use of a new IoT ecosystem, which has culminated in every cybersecurity measure having an impact on everything else on the network.

Even if physical security is run on a separate network from


Roy Alves

the corporate IT infrastructure (an impractical and expensive solution) human beings are fallible: an inadvertent connection to a broadband router; an accidental cross connection in a wiring closet or any number of unintentional oversights. In the face of all these challenges, how do you develop an effective cybersecurity strategy?

Securing an interconnected web of systems

The solution is to find an optimal way of merging the best practices of both the physical security world with the best practices of a traditional IT domain, without introducing new cybersecurity vulnerabilities for other components in the converged system.

In a converged ecosystem such as an IP-based physical security scenario, the cyber threats and vulnerabilities become far more complex. Not only does the number of components

increase, so do the number of vendors that are supplying that technology and the number of users accessing them. To mitigate risks in this kind of an open ecosystem, you need all the vendors operating off the same cybersecurity playbook.

Finding common ground to mitigating cyber risks

IT, physical security and technology manufacturers should be working as a cohesive unit – reaching consensus on current standards and current cyber mitigation technologies that really reflect "Highest Common Denominator" cyber risk mitigation techniques.

In most cases, the video surveillance cameras and video management system (VMS) are selected on two main criteria: their specific intended use – perimeter protection, surveillance in crowded public areas, etc. – and the strength of the vendor to satisfy that specific use. But there's a third criteria that needs to be considered as well: does Camera Manufacturer A support the same security protocols as VMS Manufacturer B and do these protocols tie seamlessly into IT's current suite of hardware, software and cyber protection protocols?

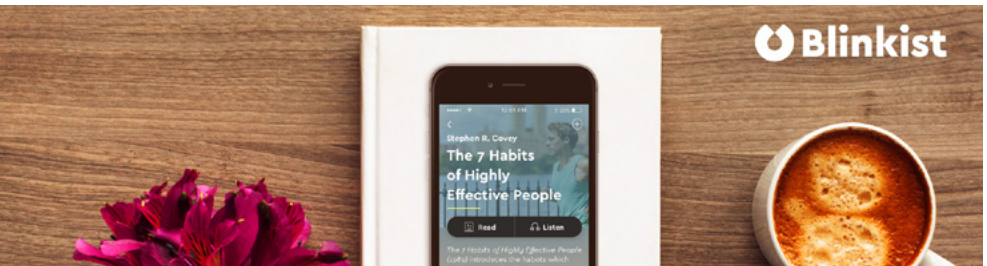
Who owns connectivity?

Since the ecosystem runs on IT's infrastructure, it raises another important question: Who is responsible for the connectivity? Do cybersecurity strategies for the physical security network-attached systems and device now belong to IT? Or does the physical security department mandate that IT support the cybersecurity technologies built into physical security's solutions? The simplest answer is that physical security management needs to work with integrators and manufacturers to devise solutions that are inherently supportive of IT's current methodologies for cyber risk mitigation.

Making sure cybersecurity is a team effort

The similarities in cyber protection technologies between IoT and physical security might be self-evident, but there are some key concerns that should remain at the forefront of any system builder. No matter how sophisticated IoT devices and systems become they still operate in an IT world. And as such, they need to adopt a cooperative cyber protection strategy. Mature IoT technologies such as physical security will need to evolve to benefit from some of the emerging IoT cyber protection techniques.

In the meantime, those in the trenches will have to understand the environment their organisation exists in and address the increasing risk of cyber threats as a joint effort between vendor, security professionals and IT. We need to work with common tools to provide the end-user with the best possible cyber protection while living within budgetary constraints.



Roy Alves, Axis Communications South Africa

CONNECT WITH ROY

Roy Alves is Country Manager at Axis Communications South Africa. www.axis.com/za/en/