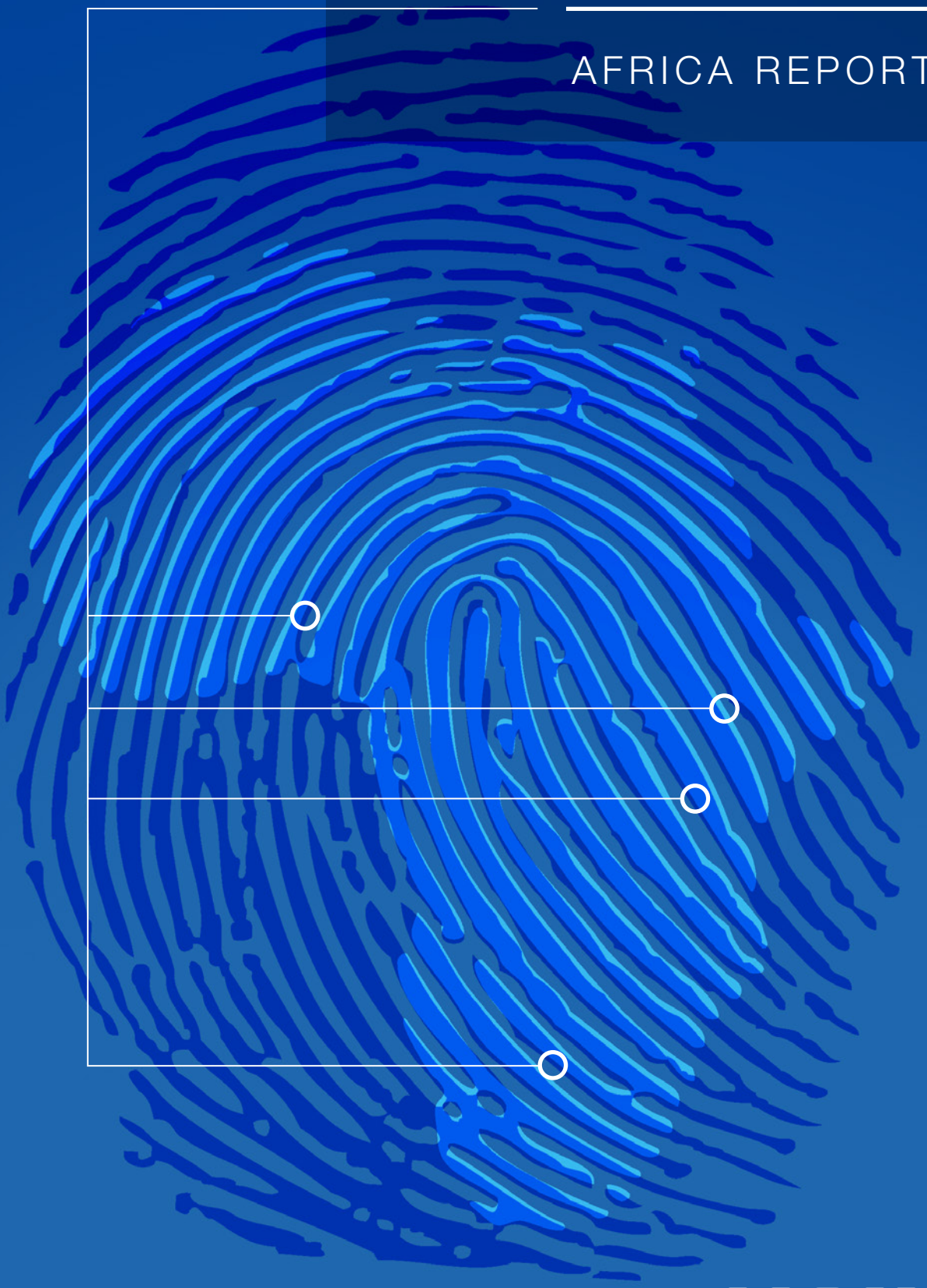
CYBERSECURITY & DATA PROTECTION

AFRICA REPORT



LIQUID TELECOM

AFRICAN.

We can help grow world-class business out of Africa.

We believe in the ambition and potential of African business. It's why we've built Africa's largest fibre infrastructure and provide an award-winning satellite network, capable of keeping any enterprise connected, protected and competitive at all times. Because we are not just a telecoms company.

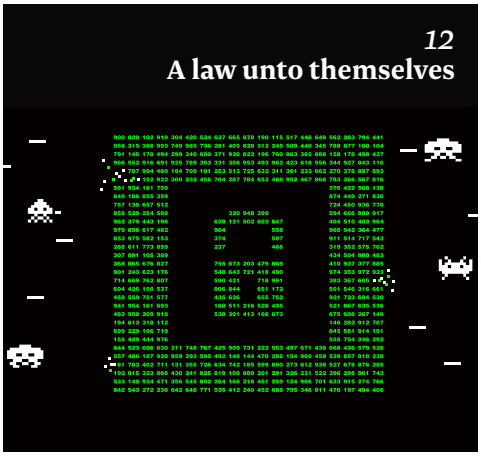
We are your technology partner.

LIQUID TELECOM

www.liquidtelecom.com

Building Africa's digital future

Contents



Preventing a cybercrime-wave

Welcome to Liquid Telecom's first report dedicated to exploring how cybersecurity and data protection are impacting businesses across Africa. In the wake of soaring internet use across the region, and the rise of the continent's digital economy, comes the threat of damaging and increasingly sophisticated cybercrime.

Incidents of cybercrime are on the increase across the region and globally, prompting the business community to raise its game or risk the financial devastation caused by a cyberattack or data breach.

Some of the figures are terrifying. As digitalisation for both consumers and enterprises accelerates, the cost of data breaches is expected to increase to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015, according to Juniper Research.

And that's just what the experts know. According to the World Economic Forum (WEF), a significant amount of cybercrime goes undetected – be it from hackers using zombie viruses or the murky underworld of industrial espionage where access to documents and data is difficult to spot (more about those later).

African businesses find themselves at a crossroads, where they must balance digital transformation with a greater focus on security policies and how to protect customer data.

Cybersecurity isn't just a technology issue. A recurring theme throughout the report is how vital the human factor is in the fight against cybercrime. People are often the weakest link in preventing cyberattacks or a data breach. Be it finding the right skills and talent to build an organisation's cybersecurity policy, or raising awareness amongst staff about basic measures they can take to strengthen operations.

This isn't just a big job for businesses, but governments across the region carry a heavy burden too – particularly when it comes to data protection. With Africa's digital economy continuing to scale up rapidly, the need is becoming more apparent for regulation and legislation to match. Approaches to the protection of data are changing across Africa, affecting both the digital privacy of citizens and the obligations of those that hold customer information.

Establishing a regulatory framework that both protects citizens and allows for healthy economic development should be the end goal for many African nations.

As in the long run, getting cybersecurity and data protection right will benefit all parties – consumers, businesses and governments alike – which is why now is the time for positive action.

> **People are often the weakest link in preventing cyberattacks or a data breach.**

Editor:
Alex Hawkes

Contributor:
Guy Matthews

Designer:
Graham Taylor

Printed by:
Law Printing (Pty) Ltd

Feedback:
alex.hawkes@liquidtelecom.com

Follow us
@liquidtelecom
linkedin.com/company/liquid-telecom
facebook.com/liquidtelecomgroup/

Clear and present danger

The fight against cybercrime looks as uncertain as ever across Africa. A new study by Liquid Telecom identifies that African businesses are under mounting pressure to enhance cybersecurity across their operations and greater fear the repercussions of a data breach.

African businesses are failing to take necessary steps to protect themselves against data breaches. Many organisations have experienced multiple security breaches within the last 12 months. The region could be facing a skills shortage as businesses struggle to find trained and qualified cybersecurity professionals.

These are just some of the concerns highlighted by businesses in new research conducted by Liquid Telecom. The study is one of the first of its kind evaluating how heavily the issues of cybersecurity and data protection weigh on the minds of employees at African businesses today.

The study exposes a lack of confidence among African businesses in combatting the growing risk of cybercrime, and indicates they are ill prepared for the fight ahead. Full findings from the survey are outlined below, with many of the key issues and themes explored further throughout the report.

Who took part in the survey?

In order to gather the data, Liquid Telecom surveyed 269 respondents from the business community. There is an even split between respondents with operations in Africa, as well as the international perspective on African business.

Respondents drew experience from a wide range of industries. Almost a third of respondents worked within the IT sector.

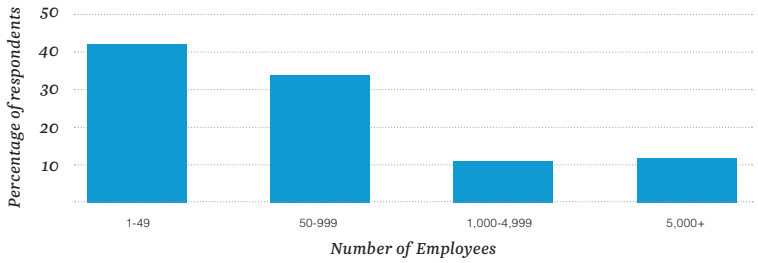
The finance community also featured prominently (making up 14% of respondents), as did telecoms (almost 9%) and agriculture, mining, manufacturing, construction and utilities (also almost 9%).

The organisation size for respondents also varies (see fig. i). Over 40% of respondents work for microbusinesses and small organisations, while just over a third are employed by small to medium sized businesses with under 1000 employees. Large enterprises with more than 5000 employees make up just 12% of respondents.

Within these organisations, a large proportion of respondents were mid-level management all the way through to c-level. Within the IT community, the survey was popular among engineers, developers and technical support.

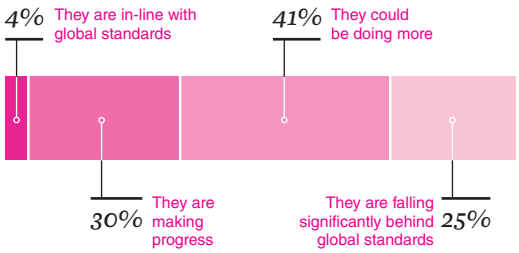
As a result, the data strikes a healthy balance between strategic overview and technical expertise.

fig. i | What is the approximate size of your organisation?



RISKS

fig. ii | Do you think African businesses are doing enough to protect themselves against data breaches?



ONTHE DEFENSIVE

African businesses are failing to take enough precaution to prevent data breaches. Over 40% of respondents (see fig. ii) believe African businesses could be doing more to protect themselves from data breaches, while almost a quarter feel the region is falling significantly behind global standards. Nearly 30% of respondents have a more optimistic outlook, believing that African businesses are making progress in the field of data protection. A small minority believe the region is in-line with global standards.

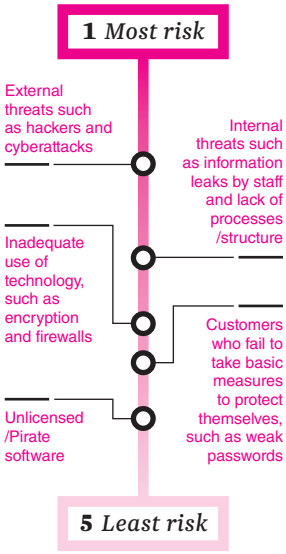
RISKY BUSINESS

Digital innovation has brought with it greater digital risk. Top of these concerns (see fig. iii) is the external threat posed from hackers and cybercriminals.

Cyberattacks are on the rise across Africa, as mobile operators, ISPs, governments and large enterprises have increasingly found themselves subject to high-profile cyberattacks. The most common and potentially devastating of these is Distributed Denial of Service (DDoS) attacks, which typically involve hackers flooding a server with thousands of requests that can knock out services. There has been a 129% increase in DDoS attacks globally since Q2 2015, according to Akamai.

But cybercrime is often closer to home than you think. Internal threats posed by disgruntled, careless or uninformed employees are the second biggest risk to businesses according to respondents. A close third is inadequate use of cybersecurity technologies.

fig. iii | Rank in order which of the following areas you see as posing the most risk to your business?



All percentages have been rounded and may not total 100%

RISKS (cont'd)

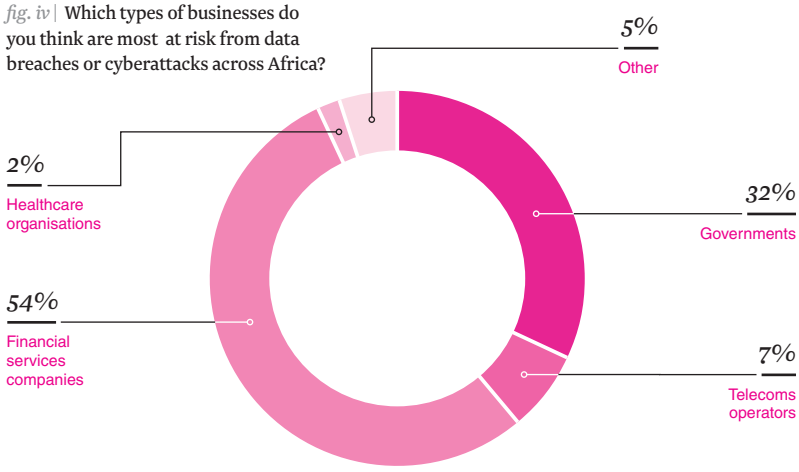
FINANCE ONTHE FRONTLINE

Banks are under more pressure than any other industry in Africa to step up their fight against cyberattacks. Over half of respondents (see fig. iv) believe financial services firms in Africa are most at risk from a data breach or cyberattack.

Meanwhile, African governments are facing ongoing and high-profile battles with the hacking community (see page 15 for our interview with an ex-hacker), which has not gone unnoticed by the business world, with almost a third of respondents selecting the public sector most at risk.

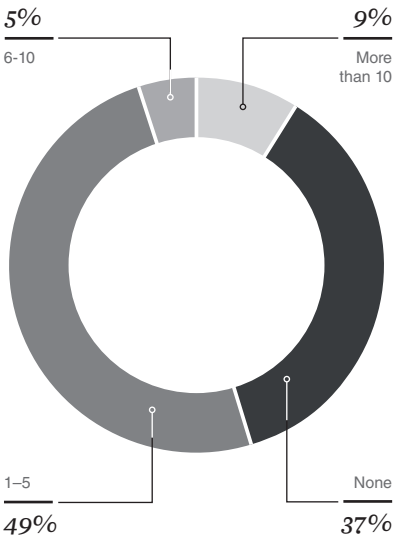
Despite some famous casualties in Europe and the US, mobile operators and other telecoms companies were selected by just 7% of respondents.

fig. iv | Which types of businesses do you think are most at risk from data breaches or cyberattacks across Africa?



ACCOUNTABILITY

fig. v | How many security breaches do you have per year?



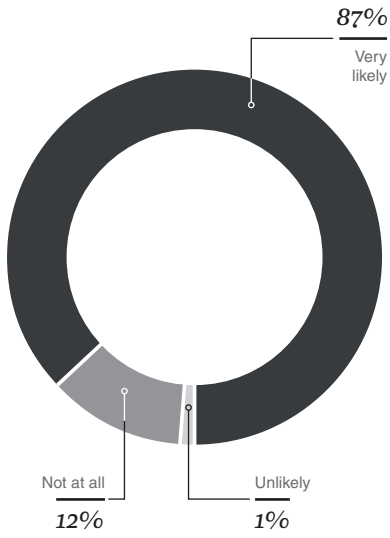
THE NEW STATUS QUO

Security breaches are commonplace across Africa. An astonishing two thirds of respondents (see fig.v) have experienced a security breach in the last 12 months.

Almost 10% of respondents claim their organisation has suffered more than 10 security breaches, while almost half state they have encountered between one and five security breaches.

In South Africa alone, data breaches increased 15% in the first half of 2016, according to Gemalto's Breach Level Index. Can organisations risk these figures increasing further?

fig. vi | How likely would a cyberattack change your security practice?



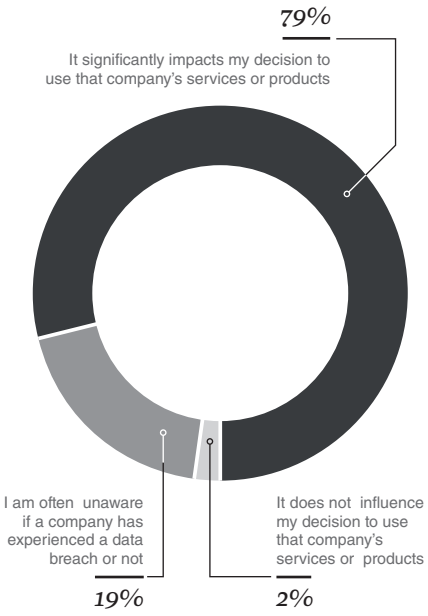
TIMETO REASSESS

Are African businesses learning from their mistakes?

Given how many respondents openly admit that their organisation has experienced multiple security breaches over the last 12 months, a major review and overhaul of existing security practices should be on the horizon.

Over 85% of respondents (see fig.vi) believe a cyberattack will prompt them to reconsider security practices and measures at their organisation. Meanwhile, only 1% of respondents believe a security breach would fail to make their organisation reassess their cybersecurity procedures.

fig. vii | How significantly do you think a data breach impacts a company's reputation?



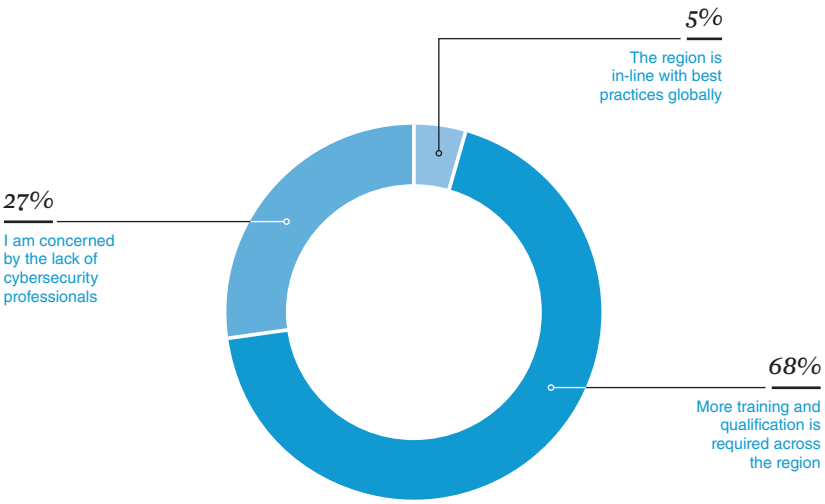
EARNING A BAD REPUTATION

How quickly would you forgive and forget an organisation if it lost your personal data to a cybercriminal? Respondents are in agreement (almost 80% in fact) that a data breach can have a dramatic impact on the reputation of its businesses among customers (see fig. vii). Perhaps more disconcerting is that almost a fifth of respondents say they are unaware when organisations have even experienced a data breach.

Businesses must adopt formal processes for reporting data breaches, with information sharing between organisations also a key component in the fight against data theft.

PREVENTION

fig. viii | Do you think there are enough skills and expertise in the area of data protection and cybersecurity across Africa?

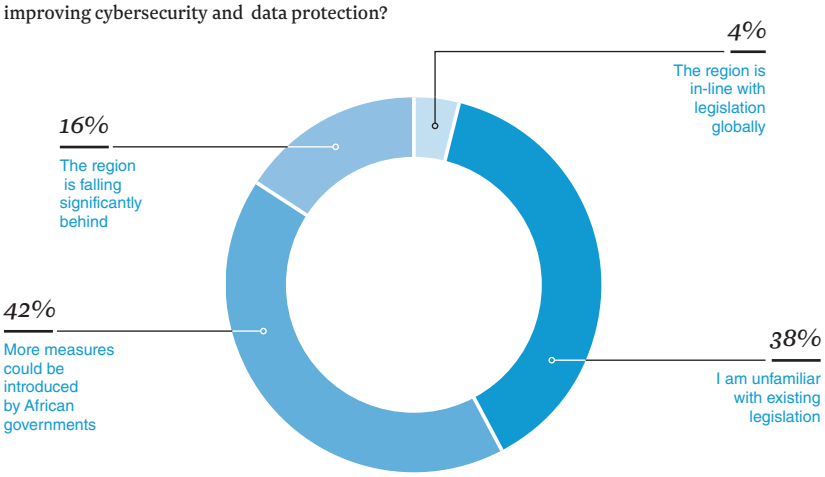


MINDTHE SKILLS GAP

A skills crisis could be emerging across Africa, with the survey results indicating there is a limited pool of cybersecurity talent (see fig. viii). Over two thirds of respondents believe more training and qualified cybersecurity professionals are required. Furthermore, over a quarter of respondents express genuine concern over the lack of qualified cybersecurity professionals in the region.

With demand for cybersecurity on the rise in Africa, filling positions could become an increasingly hard process for businesses. From entry level through to senior leadership, businesses should begin exploring how to develop the next-generation of security professionals (turn to page 6 for our full analysis on the skills shortage facing African businesses).

fig. ix | Do you think there is enough legislation in place across Africa to support businesses in improving cybersecurity and data protection?



AN ALARMING RESPONSE

It is difficult to determine which is the more alarming statistic: the fact that over 40% (see fig ix) of respondents believe African governments should be introducing tougher legislation to support businesses in their fight against cybercrime, or that almost 40% aren't even familiar enough with existing legislation to fully answer the question. What is clear, however, is that data protection legislation is a grey area for many businesses across Africa. Data protection legislation is evolving quickly across the region and businesses must keep up (see page 12 for more detail).

All percentages have been rounded and may not total 100%

PLENTY OF ROOM FOR IMPROVEMENT

Finally, we asked the market what improvements they would like to see over the next 12 months to enhance cybersecurity and data protection across Africa (see fig x).

Much work lies ahead by the looks of things. And top of the pile is investing further in cybersecurity training, reiterating earlier concerns that a skills shortage is emerging in the region.

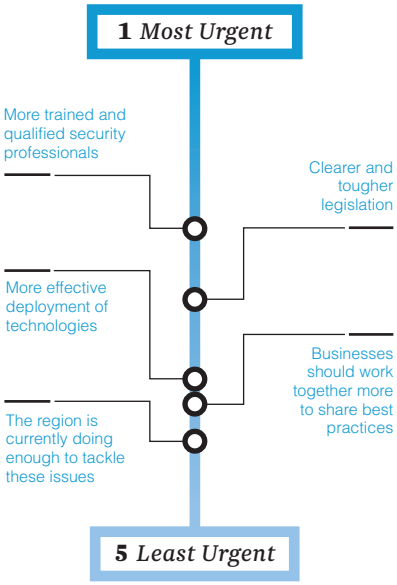
Governments also have their work cut out, with clearer and tougher legislation from governments coming a narrow second.

More effective deployment of cybersecurity technologies also scored favourably among respondents. Must haves include anti-malware, firewalls, authentication and authorisation, network access control, and intrusion and prevention systems (see Smart Security Tips on page 9 for more details).

Greater collaboration between businesses also scored strongly. Industry alliances and conferences are an effective way for businesses to regularly meet and share best practices.

Only a small minority of respondents think the region is currently doing enough to counter cybercrime.

fig. x | Rank in order which of the following you would like to see prioritised in Africa over the next 12 months to improve cybersecurity and data protection?



The new generation of African cybercrime busters

Africa is facing a major shortage of IT security professionals with the skill sets needed to tackle the continent's surging number of cyberattacks. How can businesses in the region help usher in a new generation of cybercrime busters?

Africa's two largest economies, South Africa and Nigeria, are estimated to be losing $500m annually to cyber criminals like hackers, fraudsters and those intent on digital sabotage, according to a recent report from security software maker McAfee.

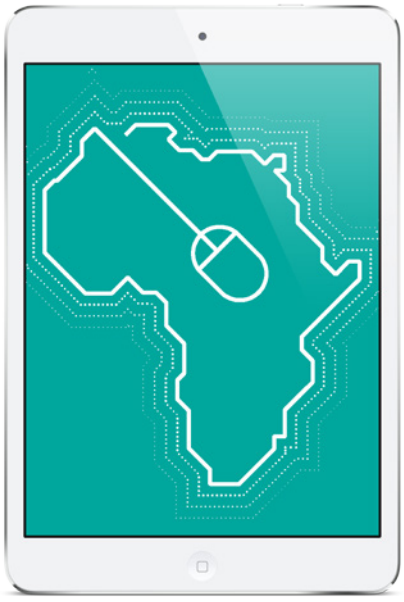
And the problem appears to be getting more acute year on year. The severity of cyberattacks in East Africa alone was 37% higher in 2016 compared with the previous year, according to independent risk consultancy Control Risks which works with a variety of clients to assess threat levels.

"Cyber criminals are getting cleverer," says Wendy Cheshire, Director of Cybersecurity with global risk and strategic consulting firm Control Risks. "They are getting better at exploiting the data they manage to steal, and they are stealing it much more adeptly. They used to just go for financial targets, like credit cards. They are now upping the ante and stealing intellectual property for sale on the dark web. They are taking data from various sources to create pots of valuable data for sale."

Confronting the skills gap

In battling this rising tide of threat, African enterprises are running into what is, in truth, a global problem – a desperate shortage of people with the right skills and experience to match the agility, resources and cunning of the cybercrime fraternity.

Neither Africa's corporate training departments nor its public education sector are producing talented people at a fast enough rate to match the evolving nature of the problem. Tough economic conditions are tending to apply downward pressure on business ICT training budgets at a time when they should be increasing, loading added pressure onto existing staff. And governments are in many cases failing to play their part by not putting enough resources into national skills development programmes. "Looking just at east Africa, there is a huge shortage of cybersecurity specialists," says Collins Oduor Onyango, IT Security Manager with Nairobi-based Strathmore University, which in 2015 launched a number of courses to deliver



AFRICAN POLICY ON CYBERCRIME AND THE ACTION BEING TAKEN TO DEVELOP THE RIGHT SKILLS

Initiatives to counter cybercrime are in evidence throughout Africa. On a continent-wide level, the African Union adopted the Convention on Cybersecurity and Data Protection in July 2014 in a bid to harmonise efforts, even if it remains to be implemented in the 53 countries which signed it. "It is good that all those countries agreed some common principles," says Christophe Fichet, a partner in the Paris office of law firm Simmons & Simmons. "There are also numerous regional initiatives in the north, south, east and west of the continent – an encouraging sign."

As well as developing policies to battle cyber threats, some individual countries are taking government-led initiatives to develop an appropriate skills base.

Morocco now has a national strategy on cybersecurity, with certifications and training developed to match. The country's officially recognised national cybersecurity framework has the aim of implementing internationally-recognised cybersecurity standards and of encouraging citizens to study for official certifications and accreditations.

Kenya has invested a lot of money to become a key ICT hub for east Africa, and that has included encouraging investment in security skills. The country has been disproportionately hit by cyber threats, as the main regional landing station for so many major subsea cable systems. But some have criticised Kenya's legislation on cybercrime and its regulation of social media as excessive and designed to stifle political opposition. **Zimbabwe**'s Computer and Cyber Crime Bill has also fallen foul of human rights watchdogs before it even becomes law.

South Africa is another of the continent's most vulnerable economies, given its relatively strong growth and performance. In South Africa, 32% of organisations have experienced cybercrime, and 57% believe they will be affected in the next two years, according to a study from Intel security. It is working on cybercrime legislation with a view to consolidate and update cybercrime provisions scattered among other laws. Meanwhile, **Nigeria** has passed a lot of law around money laundering and cyber theft. "We're seeing some smaller countries, like **Cameroon** and **Cote D'Ivoire**, developing interesting cybersecurity policies," says Fichet. "There's also proactive cybersecurity legislation in **Benin**, **DR Congo**, **Zambia** and **Chad**, all as active in this area as the big economies like South Africa and Nigeria. They want to be seen as a good place for business and a place where business is protected, and governments are legislating for this."

high level cybersecurity training. "Kenya has a particular problem because the number of internet users has increased so dramatically over the past few years as people get more dependent on using mobile technology to access it. At the same time, organisations are automating their systems and providing more services online."

Onyango says the cybercrime skills gap is one of the major concerns for businesses in Kenya and the wider region: "It's a challenge not just for corporate organisations, but government ones too," he explains. "Both are centre stage in this cyber warfare and do not have the resources to protect their assets."

Strathmore is turning out approximately 1,000 IT graduates every year, about 500 of which are trained in cybersecurity. "We're dealing both with students who enrol themselves, and people sent to us by their companies to learn," says Onyango. "We have vacancies, and we want to work closely with industry to make sure we get more students. Not everyone is aware of our potential and we want to reach out to them."

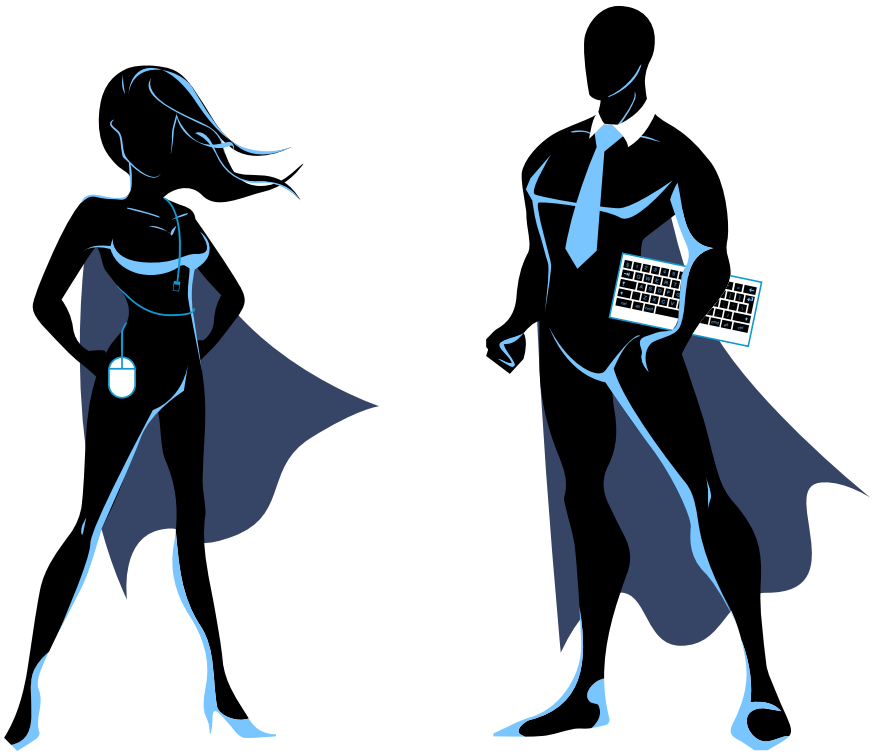
Onyango believes that fighting cybercrime makes for an attractive and exciting career: "There's a lot of learning to do, as technology keeps changing and so do vulnerabilities," he says. "The threat landscape keeps evolving. Cybersecurity has a big future as we move more into cloud and Big Data."

A 'cool' career choice

As well as taking advantage of the growing number of available courses and certifications, organisations can be doing more internally to support the development of cybersecurity skills.

They can establish clear career paths for cybersecurity professionals, supported by ongoing training and internships. They will naturally have to take onboard the obvious risk that a trained professional can easily leave at any time for a better paid job. But if that person can see room for career development, they might elect to stay. Industry should also work harder to diversify the pool of potential security professionals it is reaching out to. Cybersecurity is a male-dominated sector, but that can and is changing says Cheshire from Control Risks: "I'm seeing a lot of women come into cyber security, perhaps business women looking for a new career or to enter a new market," she observes. "They bring a lot, being intuitive, collaborative, inquisitive and adaptable – all the qualities you need in cyber security. They are good in fields like cultural change and strategic thinking. Organisations need to realise they don't just need to be going for that very stereotypical male hacker type with his balaclava, or the young male IT geek either."

Not all cyber threats are purely technical, and available careers should reflect that: "One of the big threats, and a largely under reported one, is insider cybercrime where someone working inside a business leaks information intentionally, or accidentally," she points out. "This illustrates the point that cybersecurity is sometimes a cultural matter. Security is a holistic business. You have to look at the culture of the organisation. How is data managed and ring-fenced? Are we looking at the problem strategically or just tactically?"



> **Looking just at east Africa, there is a huge shortage of cybersecurity specialists.**

Schools too can work harder to position cybersecurity as a 'cool' career, and offer more hands-on training. A survey by Intel Security found that hackathons were an effective way to identify talent and develop skills.

A fight on all fronts

While cybercrime is not an exclusively African issue, it does demand a concerted African approach at the highest possible level if the continent's digital economy is to continue to flourish: "You've got companies like Liquid Telecom laying fibre, and now we are ready for the next layer, the services," says Christophe Fichet, a Partner in the Paris office of law firm Simmons & Simmons. "If the continent wants to make a full digital transition and move to digital business, and attract big companies like Google that want to come to Africa, then there is another challenge."

Africa needs legislation and sanctions to create an environment that favours this digitalisation. The catch is that you can make all the legislation you want, but you need people to make it work. "It is complex technically to fight cybercrime, and you need people who really understand it before you can regulate and legislate successfully."

Given a concerted effort on all fronts, then Africa will soon have a new generation of security professionals to answer Fichet's call, and to staff the front line in the fight against digital wrongdoers.

The growing pains of devices in the workplace

Bring Your Own Device (BYOD) is already a security incident waiting to happen for many businesses. But in Africa, where many employees own multiple devices, the risks are stacked even higher.

Daniel Cuthbert
COO, SensePost

The era of desktop computers both at home and at the office never really happened across Africa. Instead smartphones became the main form of accessing the internet, and today many people in African countries have multiple devices on them at any given time.

As a result, demand for BYOD at offices in the region has soared as many employees bring two, three or sometimes even four devices with them to work. This can make the task of securing internal networks even harder for organisations. Particularly when employees fail to keep their devices updated.

Mobile data can be expensive in many African countries, and many consumers put-off updating apps or their device's operating system in order to conserve valuable data. Older device operating systems – particularly Android 3 and 4 – are less secure, and so consumers are putting themselves and their organisations at risk by not updating.

Same goes for app updates. I cannot tell you how many times I have shoulder surfed and seen dozens of update icons on somebody's device screen. I understand why someone would rather be using their phone than updating it, but attackers do abuse that. Businesses need to accept that employees will be bringing in multiple devices and give them the means to use those devices in a secure manner, or be more draconian about it and instruct them not to use personal devices inside the work environment. I favour the former; provide a dedicated Wi-Fi network for internal use and raise awareness about device security. Things employees should be watching out for include malicious apps lurking in app stores (less so in the Apple app store, but more so in Google Play) and malicious hotspots.

> **Provide a dedicated Wi-Fi network for internal use and raise awareness about device security.**

Rogue apps are a particularly strong concern for banks, with a few big names in the business caught out by subtly altered versions of popular banking apps appearing in app stores, which lure customers to part with mobile banking passwords.

We live in a world where you go somewhere and immediately look for the nearest Wi-Fi network. But using a public Wi-Fi network brings with it risk – the network could also be used by compromised devices or the hotspot itself could be malicious.

Wi-Fi fraud is simple and easy to do, so too are the man-in-the-middle attacks against older apps which don't have such good security.

These attacks are made out to be sophisticated but in reality they are not. Look at what happened to TalkTalk in the UK, which lost personal data from over 150,000 customers during a cyberattack. The organisation didn't take basic steps to protect itself and the hacker turned out to be a 15 year old boy who didn't really know what he was doing. It's hugely embarrassing.

And because there has been no real push to make it mandatory for organisations to report these types of fraud or data breaches, it is hard to quantify the number of attacks.

But from what SensePost is hearing, consumers are getting attacked and it is easy for attackers to exploit information and gain access to money.

Raising consumer awareness is important. In the UK, Barclays has recently launched a video campaign which clearly explains to viewers what details a bank might ask for and what details a fraudster might ask for. It's a refreshing approach which banks and other organisations in Africa could learn from.

Security is often the last thing businesses think about. They don't assume criminals are after their information. They are and businesses need to be much smarter with how they handle customer data.

Smart security tips for your business

From preventing your business being held to ransom by malicious software to simply reminding your staff to update anti-malware on their devices, Liquid Telecom gives its smart tips for strengthening security at the workplace.

Make use of what you already have

Minimising risk doesn't always require the latest and greatest cybersecurity technologies, some of the fundamentals are available at the click of a button. Encryption, for example, is such a basic principle for protecting sensitive data that some businesses forget to even activate the technology.

Encryption converts data into cipher text making it only accessible by secret key or password. For Mac users, activating the file encryption tool, FireVault, instantly converts your start-up drive from its unencrypted state to fully encrypted. Once the conversion is complete, you have a fully protected drive that only you can access or even erase remotely in case of theft using the Find My Mac app. Microsoft has a similar system called BitLocker. Encryption is sometimes a default on Windows 10. And sometimes it is not so make sure to check. Android devices traditionally did not come with encryption services activated, but this was rectified last year with the arrival of Android Lollipop 5.0.

Password management is another simple but effective form of instantly strengthening security at a business. No matter how much embarrassment has befallen celebrities whose weak password choices has led to compromising pictures catapulting across the internet, passwords are still given very little time and attention. Analysing over 2 million passwords leaked during 2015, SplashData found "123456" and "password" to be the top two most commonly used passwords. Weak and easily guessable passwords are a wide open door to hacking and identity theft and can be easily addressed by avoiding words in the dictionary (use a compound instead) or by making good use of free password management tools available online.

Educate your employees

You're only as strong as your weakest link is the message every CIO should be telling employees.

Raising awareness amongst staff isn't a difficult or daunting task: they simply need to know some of the risks and some of the steps they can take to minimise them.

Most employees are aware by now of the existence of malware – probably because they've learnt the hard way at home.

Remind them that the simple steps still apply at the workplace: make sure anti-malware, operating systems and other programs are kept updated. Most staff are most likely to also be aware of phishing emails and scams (read more about them on page 10), but extra diligence is required in the workplace as is the need to report suspicious emails to a relevant member of the IT team.

As well as preventing malware and alike getting in, businesses need to make staff aware of the risk of sensitive information getting out. A secure file transfer system should be used to send any confidential information externally.

Preventing unauthorised access can be as simple as reminding employees to lock their screens while away from their desk, or physically locking their work laptops away when not in use.

The proliferation of bring-your-own-device (BYOD) has opened up more holes for confidential information to pour out of. Dedicated Wi-Fi for personal devices and greater user awareness of maintaining operating system and app updates can go a long way to counter this (turn to page 8 for more information).

Finally, organisations themselves have to account for human error. Mistakes after all will happen.

Don't get held to ransom

Ransoms are no longer just for multi-millionaires or bad movies starring Mel Gibson. Any business could find itself blackmailed these days, thanks to a particularly malicious bit of software known as ransomware.

In a nutshell, ransomware prevents or limits users from being able to access their systems by taking control of a target's computer and then encrypting all the data on it. The software's developer then demands a payment in exchange for handing over the encryption keys.

The first incarnation of ransomware appeared online as early as 2005, and since then, ransomware figures have grown rapidly year-on-year. According to Kaspersky's IT Threat Evolution Report, the security firm detected 2,900 new ransomware variants in Q1 2016, which shows a 14% increase compared to the previous quarter.

Businesses in particular should be aware of rising numbers of mobile ransomware, with Android devices being a particular target. Windows-based devices are at threat from a new version of CryptoLocker, which now encrypts file names along with data, in order to make it even harder for victims to recover data, according to Kaspersky. Ransomware victims aren't just large organisations, home users and SMEs are equally just as at risk – schools, hospitals and churches have all been struck. Ransomware can be extremely profitable. According to a 2015 report from Trustwave, criminals can get an estimated 1,425% return on investment for their ransomware operations, with the average ransom demand being between $300 to $500.

Bitcoin has played an unwilling role in the rise of ransomware, with many cybercriminals demanding payment in the digital currency. Scared businesses are even thought to be stockpiling bitcoin in the eventuality of a ransom.

There is a simple and effective solution for businesses to ransomware that doesn't involve handing over large wads of money to cybercriminals: backup your data. "If all your local drives and computers are backed up 24/7 then the extortionists pose no threat to your business," says David Behr, Chief Product Officer at Liquid Telecom. "CrashPlan is a great example of how you can resolve this issue."

Time to sink or swim with phishing

You don't need to be an evil IT mastermind to persuade someone to hand over sensitive information. In fact, cybercrime these days is as much about social engineering as it is malware and viruses. As businesses have looked to address technical deficiencies, hackers have found a new weak spot in humans. And in phishing, pharming, vishing and smishing, fraudsters have some effective weapons in their arsenal to choose from.

Phishing is an attempt to fraudulently obtain sensitive information – be it credit card details or bank account information. The message is typically formatted to disguise itself as a legitimate request from a credible source. According to a study by the Anti-Phishing Working Group, phishing activity rose an astonishing 250% between October 2015 and March 2016. Traditionally, phishing has been low-end scammers who have cobbled together an email full of warning signs, such as overly formal greetings, bad grammar and the promise of fame and fortune. Not anymore. Today's phising emails are carefully crafted and targeted at the end user, usually referred to as "spear phishing" and if the target is a senior executive, "whaling". They may know your business or your personal interests. They may have obtained this information by visiting a company's public website, observing and extrapolating the company structure using business focused social media tools, but this knowledge can lull users into trusting the message. Businesses can ensure such messages are prevented from reaching staff by deploying an effective email management system. These types of threats are not only consigned to emails. Staff also face potential scams via phone call (vishing) and via text messages (smishing).

Also beware of phishing's evil twin pharming. This time instead of a bogus message, pharming uses a bogus website to trick users into entering personal or sensitive information. As well as teaching staff to avoid suspicious looking links and websites, protection against these types of attack includes a strong antivirus and antimalware solution.

Cloud on the horizon

If you believe the hype, a corporate "no-cloud" policy could be as rare as a "no-internet" policy in the not-so-distant future. According to Gartner, more than $1 trillion in IT spending will be directly or indirectly affected by the shift to cloud over the next five years

Most businesses have indeed woken up to the advantages of cloud: cost savings, agility and innovation to name but a few. Cloud can help organisations build a modern IT environment, providing them with a platform to build their digital business and future applications. But at the same time it does effectively mean you're handing over the keys to your Mercedes Benz to a cloud provider.

Even though cloud environments face the same threats as traditional corporate networks, they are a particularly attractive target given the vast amount of data stored on cloud servers. And cloud hacks do happen – with some of the biggest names in the business such as Apple and Amazon having fallen victim to hacks. To counter this, most organisations should be using a combination of cloud services from different cloud providers. They should also be exploring hybrid cloud environments, in which businesses mix private and public cloud services with orchestration between the two platforms.

Meanwhile, cloud-based services are also becoming an increasingly favoured option for businesses to bolster cybersecurity. Unified threat management is a great way to combine all your cybersecurity needs - be it firewall, network detection, antimalware, spam and content filtering or VPN capabilities – into one integrated package. This gives businesses advanced control over installation and updates, reducing overall complexity.

But again the flipside can be that it puts businesses at risk of a single point of failure.

"Take advantage of cloud offerings on the market, but do your homework and mitigate the risks," says Behr. "Using a product like CrashPlan means all your files are backed up and your business isn't reliant on one service provider."

A law unto themselves

Data protection legislation is changing fast across Africa, as governments try to balance the rights of citizens to digital privacy and security with encouraging national, regional and international commerce. It is imperative businesses keep up with these developments.

Data protection legislation in Africa can be divided into three camps: the haves, the have nots and the in-betweens. Some progressive African governments have already charged ahead with new data protection laws in the past few years, regulating the collection and use of personal information by the private and public sector. Others are on the right track and are in the process of drafting legislation or establishing bills that will control how data may be handled but which have not yet passed into law (see Data Protection Legislation To Watch). While some lag precariously behind and are yet to adopt specific measures to safeguard data, or even establish a national protection authority of any kind.

As well as protecting the digital privacy of citizens and outlining the obligations of the businesses that hold customer information, effective data protection legislation can have a big say in the future health of an economy.

Governments without effective means to safeguard and regulate data may be endangering future foreign investment, not to mention relegating their citizens to the fringes of the global economy.

Developments to data protection legislation could be a deciding factor for businesses looking to expand across Africa, as they aim to avoid places where the integrity of data is set at a low premium, or where they might get hit hard by protectionist and maverick data laws designed to seal borders and favour indigenous enterprises.

It is in everybody's interest to come up with a healthy data protection environment.

Lessons from the EU

There are many who argue what Africa needs above all is a harmonised, pan-African approach to data protection, such that data is able to flow seamlessly across borders without falling foul of hostile regulation, all while being afforded a uniformly high level of security. The model here is clearly the European Union.

In Europe, an EU-wide data protection framework has recently been agreed between member states, offering a measure of harmonisation. The General Data Protection Regulation (GDPR) places a number of obligations on data-reliant organisations, who now know what rules they face where ever they or their data may reside within EU borders.

The GDPR will replace all current measures, most likely coming into full force in the first half of 2018. It is a clear step towards a digital single market, and a sound platform for individual countries to base their own legislation on. US law on data protection and privacy has also been tightened. The Stored Communications Act became law in 1986, but has now been clarified and modernised by a number of legal rulings.

It is very early days, but the first steps towards a harmonised African approach were taken in June 2014 with the African Union's Convention on Cyber Security and Personal Data Protection. Some 53 African states came together to agree a legal framework to regulate various fields of ICT activity, ranging from e-transactions and personal data protection to cyber security. The convention is

not however any kind of legally binding instrument, and requires that individual countries put its principles into their own statute book. To date the convention remains unratified, but offers a tantalising prospect of a unified African data policy to rival the EU and US.

Danny Preiskel, Senior Partner with law firm Prieskel & Co, believes that in the longer term Africa will increasingly feel the necessity of moving towards a European-style data protection model.

"It will happen in time," he says. "It will be needed to support things like mobile banking, which is so much more important in Africa compared to other parts of the world. It is in everybody's interest to come up with a healthy data protection environment."

Carefully assessing African markets

There is concern that a minority of African governments could be considering mirroring Russia's stringent data localisation law. Russian law mandates that if an organisation is processing certain types of personal data, then it has to be physically located on servers within the country.

"This trend, if followed, could mean that companies which rely on data will need data centres in multiple countries, whereas they might have managed with one," warns Mike Conradi, a Partner with UK law firm DLA Piper.

"This could add quite considerably to the expense of doing business in Africa, which in turn might not be a good thing for African consumers. And it might put less well-resourced companies off establishing data-related services, other than in one or two countries."

Organisations looking to do business in Africa need to carefully assess the data protection situation on a country by country basis, warns Christophe Fichet, a Partner in the Paris office of law firm Simmons & Simmons.

"In Europe you have a lot of coordination and cooperation between countries, whereas in Africa at the moment you don't have that," he says. "It's more on a country by country basis. Ideally data protection needs to be more integrated. Harmonisation of policy is important. Most countries at least are now theoretically committed to the delivery of a good level of data protection."

Not throwing caution to the wind

While African data law remains unharmonised, organisations looking to do business across borders should do so with caution.

In particular, businesses looking to take advantage of cloud-based services may need to transfer personal information between African countries, or indeed move data in and out of Africa via the US, Asia or Europe. These organisations need to ensure that every country they move data through has appropriate laws to keep it secure. Businesses also need to be certain that data is able to flow legally back out of a country once it has been routed there. And they need to be clear on the legal burdens placed on them and the network operator they use, country by country, including any criminal and civil sanctions for violations.

As ever, the price to be paid for not complying with data law can include reputational damage, loss of customers, the payment of damages following a civil class action or fines.

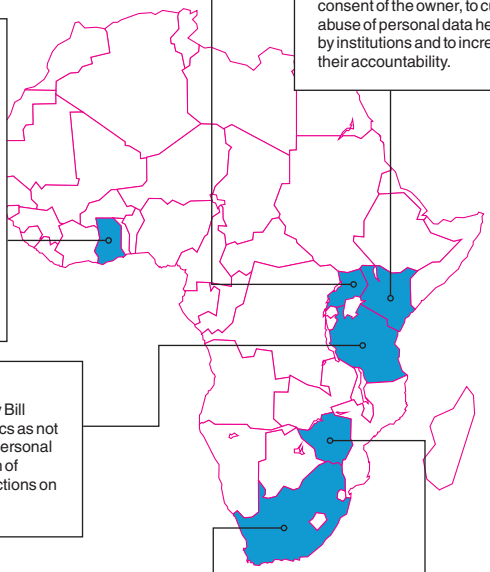
At this stage of its evolution, African data protection is still fragmented and immature, but is evolving fast and for the most part in encouraging directions. There still needs to be more consensus on the meaning of key terms like 'consent', 'public interest' and 'legitimate grounds'. But there is hope that such details can be thrashed out and enshrined in a binding framework that both protects citizens and allows for healthy economic development.

DATA PROTECTION LEGISLATION TO WATCH

UGANDA
The country's Data Protection and Privacy Bill (2014) is intended to mandate how organisations like telecoms service providers, insurers, hospitals and schools can retain and use the information of citizens. Human rights campaigners have said that the law, if passed in its current form, gives the Ugandan government too much leeway for surveillance of citizens.

KENYA
The Data Protection Bill of 2013 guarantees all citizens a right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily revealed. The aim of the act is to make it difficult for organisations to access or mine personal information without the consent of the owner, to curb abuse of personal data held by institutions and to increase their accountability.

GHANA
The Data Protection Act was adopted in 2012, with principles similar to the OECD Guidelines and the European Union Data Protection Directive. A regulator has been appointed, but adoption has been slow and has faced several challenges. The Data Protection Commission has been working to raise awareness and increase compliance.



TANZANIA
The Data Protection and Privacy Bill 2014 is considered by some critics as not going far enough to protect the personal information of citizens, and even of appearing to place undue restrictions on freedom of expression.

SOUTH AFRICA
The country's Protection of Personal Information Act (POPI) sets conditions for how organisations can lawfully collect, process and store personal information. The act was signed into law in 2013, and an information regulator was established in September 2016, but as of the time of press, a full commencement date for POPI is yet to be confirmed.

ZIMBABWE
The protection of privacy is enshrined in Zimbabwe's constitution, although as yet there is no official national legislation dealing with data protection for citizens. There are certain laws that relate to very specific types of data, and which regulate the use of personal data by public bodies.

Physical network security: dig it deep or hang it high

Investing heavily in cybersecurity but failing to physically protect the equipment itself is a bit like leaving your house with the alarm on but the backdoor wide open.

Ben Roberts
CTO, Liquid Telecom &
CEO, Liquid Telecom Kenya

Businesses face a huge challenge in protecting networks from cyberattacks, but consider for a minute some of the complexities involved in physically protecting network and ICT infrastructure. I am responsible for the network operations of the largest independent pan-African fibre network. For Liquid Telecom, our physical security requires meticulous planning to minimise the risk of fibre cuts or theft of network equipment. In a nutshell, our tactic is too dig it deep and hang it high. Our fibre can either be found 1.2 to 1.5 metres safely tucked away underground, or at the very top of utility poles running alongside electricity lines.

Other operators in the region are deploying fibre as fast as they can, but sometimes at the cost of leaving their networks exposed. In several cities I have visited there are many cases where the wires have sunk so low from the pylons that anyone could come along and grab hold of them or inflict accidental or malicious damage.

There are some incidents that are hard to avoid, however. Contractors digging up roads, for example, may accidently hit and damage fibre – often reburying them and running away shortly afterwards. Or criminals sometimes venture down manholes and destroy fibre during a misguided quest for copper. Most ICT and telecoms networks will have different levels of site classifications requiring different levels of security. The architecture of any modern big network is highly distributed. And naturally leads to 3 or more levels. At the core or central office sits the data centre, at branches or network nodes sits networking equipment to connect users to the central office, and at the edge are the devices which access the network.

The impact of failure or data loss at data centre level could leave a whole country or business affected by service failure, and so these are our most secure sites: electric fencing, full CCTV coverage, armed guards, access control finger readers – the full works. The impact of failure at a branch office could impact service availability across an entire region or location. Security remains high at these sites, which are monitored by CCTV and security guards. The impact of failure from an edge device will only impact a user or small group of users. Edge devices can include network CPE devices, laptops, smartphones and point of sale devices. Here edge switches are kept under lock or entrusted to specific individuals. Theft may have minimal impact on business continuity but can result in large amounts of data loss if devices localise data that is not encrypted and backed up to the central office.

> **The architecture of any modern big network is highly distributed.**

Network infrastructure is generally not the most obvious target for criminals, but the growing threat of terrorism is changing attitudes to protecting physical infrastructure. Deadly terrorist attacks across East Africa have prompted businesses to invest further in physical security across their operations. In 2006, I was working in Nigeria alongside an engineer, who asked me to wait in his car while he went to attend a quick job at a bank. He wasn't quick and after half an hour, I decided to go and find him. I strolled through the building into the room where the main core banking servers were located to find the engineer. The firewalls in the racks remain to this day some of the largest I have ever seen. But I was able to walk straight up to them without a single person asking me for ID.

All that investment in protecting the networks from cyberattacks, without giving a second thought on how to secure the equipment itself.

This would never happen anywhere in the region today. Over the last ten years, businesses have woken up to this kind of vulnerability – be it more down to fear of a criminal brandishing a gun rather than one with a memory stick hidden up their sleeve. But it still serves as a valuable lesson to businesses: investment in the latest cybersecurity technologies should always be matched with investment in the physical protection of your equipment.

Inside the mind of a hacker

Only by understanding the mind-set of a hacker do businesses stand a chance of taking them on at their own game. An ex-hacker reveals the psychological warfare that goes on behind hacking.

From activists to anarchists, today's hackers are motivated by a multitude of different beliefs and causes. Which can make predicting their next move very tricky indeed.

What better way to understand more about the mind-set of a hacker than by interviewing a former one? This ex-hacker requested to keep his identity anonymous, so for the purposes of this interview will go under the name SoundByte. "Hacking is a community made up of millions of hackers each with their own philosophy. But somewhere along the line, some of those philosophies began to converge," explains SoundByte.

The hacking scene has evolved enormously over the last three decades. The formative years of hacking in the early 1990s were characterised by underground communities of hackers, who as well as pioneering the first hacking tools and programs, formed their own set of rules and principles. "Hacking in the 1990s was all about exploration. Yes, back then hackers did some nasty malicious things, but they wanted to learn. It was a tight knit community," says SoundByte.

This spirit of discovery was best summed up by a short essay published in 1986, now more commonly known as the Hacker Manifesto. It's a poignant reminder of the antiauthoritarian and outsider roots of hacking: *"Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for."*

Entering the mainstream

Yet as the world became increasingly digital, hacking became less of a counter culture and entered the mainstream. New hacking groups were formed.

The rise of hacktivism, for example, has seen high-profile loose knit groups such as Anonymous disrupt services for a political or social cause.

From Wikileaks to the Arab Spring, Anonymous has had a big say in global affairs over the last decade. A watershed moment came in 2008, when Anonymous became infuriated by the Church of Scientology for removing embarrassing footage of Tom Cruise from Youtube. As well as the usual online sabotage, Anonymous went overground and also organised protests and demonstrations outside Scientology centres worldwide. "Everyone at this point thought that hackers lived in their mother's basements and no one would show up. But thousands did. We realised there were many of us and we have power."

Disgusted by the social conscience of hacktivism, anarchistic hacking groups such as LulzSec emerged. With a tagline of "Laughing at your security since

2011", the group was responsible for major hacks into the servers of high-profile companies such as Fox Television, Nintendo and Sony. "They went on a cyber rampage to counter this new socially conscious movement."

Pulling the tiger's tail

Regardless of the cause, hackers are merciless in their attacks. Examples of individuals or organisations pulling the tiger's tail and living to regret it are numerous.

Aaron Barr, who was at the time CEO of HBGary Federal; a security contractor for the US government, bragged that he could use social media to gather information about hackers. Anonymous responded by not only compromising the HBGary website, but allegedly also wiping Barr's iPad remotely. "Governments and businesses even to this day have been slow to understand the cyber world. It has come to a point where they are so behind the technology that they may never be truly ahead of the hacking community."

As the stakes have got higher, the business community has increasingly turned to hackers for guidance and advice on cybersecurity. SoundByte is one of many who has made the switch from underground criminal to cybersecurity expert. "I realised I could carry on playing games or I could go make money," says SoundByte.

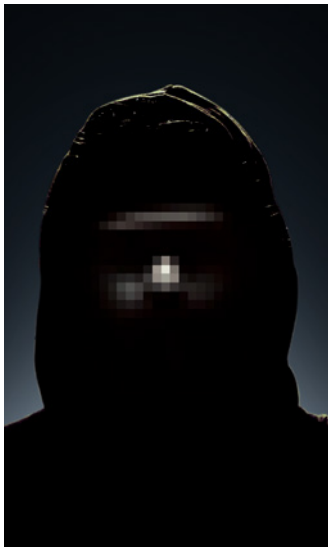
"A large number have made that jump. I recognise a lot of hackers from the mid 1990s who now are in very senior positions."

Employing an ex-hacker can give organisations further insight into the psyche of the hacking community: "Understanding the mentality of a hacker goes a long way in protecting your business. If you wanted to be better protected, go hire a hacker."

Just as some hackers have made money by joining the business community, others sell their services illegally on the dark web. Industrial espionage is more common than you may think: "You can buy denial of service online. You just need to know where to look," SoundByte says. "A competitor could buy this service and take your business offline."

Hacking can be a highly profitable occupation. As well as becoming hired mercenaries, hackers are also making a small fortune from malicious software such as ransomware (see page 10 for more details), Remote Administration Tools (RAT); programs sold by hackers that enable control of another computer remotely, and zombie viruses; which lets a hacker secretly infiltrate a victim's computer and use it to conduct illegal activities such as DDoS attacks.

Hackers are finding huge demand for bankcard details, with hacked credit card fraud expected to reach $4 billion this year and grow to $10 billion by 2020, according to a study by research firm Aite Group. Hackers are even finding that they can earn money teaching by posting tutorials on discussion boards to novice hackers.



> If you go up against the hacking community, you might be walking into a gun fight holding a tea spoon.

New battle lines

SoundByte strongly believes that the biggest threat to a business comes from within. "The reality is that most security breaches are from the inside going out. Companies often forget about protecting systems internally and it is easy for people to copy whatever they like and then sell it."

A case in point being world famous whistleblowers Chelsea Manning and Edward Snowden; who between them were responsible for leaking classified information from the US military and National Security Agency. Both were inside jobs. Social engineering, argues SoundByte, is also a key attribute of a hacker. "A major weapon in a hacker's arsenal is the ability to get someone to give you access to something," says SoundByte. "There are a lot of hackers out there exploring complex systems to help get them access. But more often than not, it is a hacker posing as someone else that secures the access."

The trick for businesses is finding a balance between deploying the latest technologies and putting in place stringent security procedures. The latter method is often the most forgotten says SoundByte. "You can put up a stack of firewalls which will block 95% of the attacks coming in, but getting the right security processes and procedures in place is the hardest part."

What tips does an ex-hacker offer businesses today? "You can't write a security policy now and leave it for two years," SoundByte says.

Seemingly simple procedures like updating firewall access can get overlooked by organisations: "If no one is constantly reviewing who has firewall access then you end up with more and more holes."

Assembling an experienced and skilled cybersecurity team is one thing, but companies often fail to mandate them with the power to take action when necessary.

"So often you have Chief Security Officers who aren't actually in power. They need to involve HR, legal teams and many other departments before they can take action."

New battle lines continue to get drawn in the murky underworld of hacking. In October, the US government officially accused Russia of stealing more than 19,000 emails from Democratic Party officials. SoundByte believes an era of state sponsored hacking is on the horizon: "The state is getting more and more involved in hacking. Governments are essentially funding hackers."

Since the Arab Spring highlighted how quickly the internet can undermine state control, governments are getting more sophisticated in their attempts to exert control online, leading to a rise in internet censorship and surveillance globally.

All of which sets the scene for ethical hackers to fight back: "Hackers don't like the state and control. They will fight against it. If you go up against the hacking community, you might be walking into a gun fight holding a tea spoon."

About Liquid Telecom

Liquid Telecom is the leading independent data, voice and IP provider in Eastern, Central and Southern Africa. It supplies fibre optic, satellite and international carrier services to Africa's largest mobile network operators, ISPs, financial institutions and businesses of all sizes. In June 2016, Liquid Telecom agreed to purchase Neotel, South Africa's first converged communications network operator, for ZAR6.55 billion, creating the first pan-Africa fibre player.

Liquid Telecom has built Africa's largest single fibre network currently spanning over 40,000km, including Neotel's network (pending approvals), across borders and covering Africa's fastest-growing economies where no fixed network has existed before.

Liquid Telecom's network provides connectivity onto the five main subsea cable systems landing in Africa; WACS, EASSY, SEACOM, SAT3 and TEAMs.

Working under various brands, the Liquid Telecom Group has operating entities in Botswana, DRC, Kenya, Lesotho, Mauritius, Rwanda, South Africa, Uganda, UK, Zambia and Zimbabwe.

The company has been named Best African Wholesale Carrier for the last four years at the annual Global Carrier Awards.

Why Liquid Telecom?

It takes an African company to really understand the challenges of connecting businesses in Africa. Liquid Telecom provides connectivity services for enterprises across many sectors. In an increasingly competitive environment, we are one of the few African operators able to use carrier-grade services to enhance network efficiency.

Suitable African partner: Given the uniqueness of Africa, it is an imperative that companies partner with a service provider that understands your requirements and can deliver against the unique African challenges.

Professional project management: Our solution will be delivered through internationally recognised project management methodologies and techniques. Our account management engagement is based on internationally recognised best-practice - with a single point of contact - thus providing engagement for both implementation and on-going service delivery.

Extensive local experience and knowledge: Our African heritage, depth of skills and extensive knowledge in the required areas, are supported by established facilities, capabilities and resources in diverse African regions. Strong local knowledge and skills ensure professional, rapid and lawful deployment.

> We're one of the few African operators able to use carrier-grade services to enhance network efficiency.

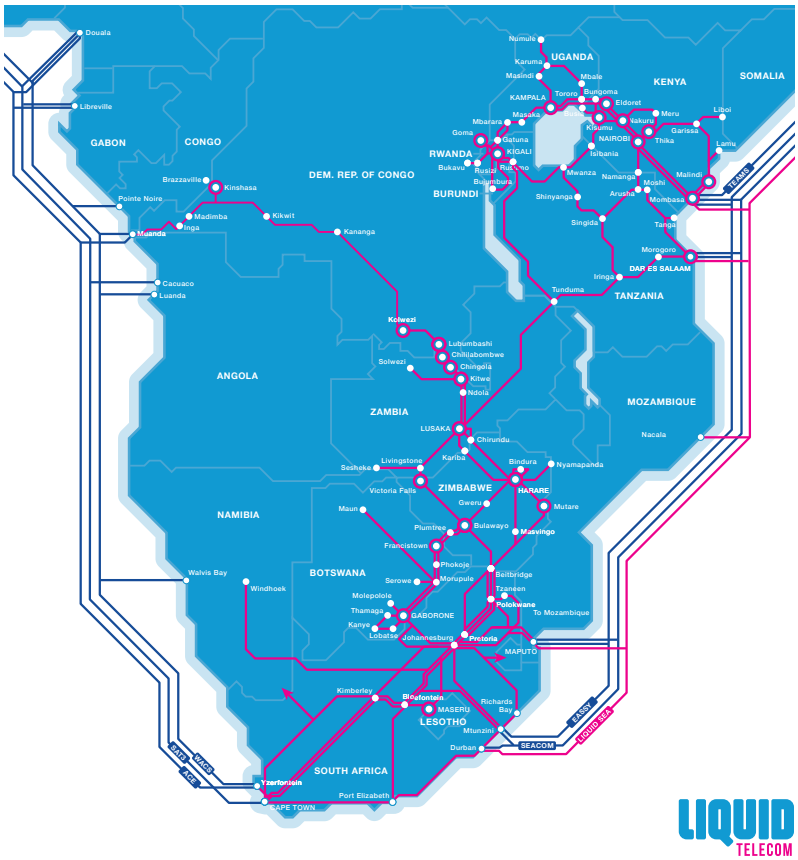
Enviable service levels: We deliver and manage multiple networks using enviable service standards through expertise in African implementations. Experience, capacity, expertise, management tools, local skills and a wide footprint ensure the achievement of these service levels.

Managed risk: Our knowledge/experience of communication services' standards and requirements ensure that our solution is to the extent that all potential risks for such a project are identified and mitigation plans crafted.

Proven ability: We help our customers to simplify communications supply chain by reducing the number of operators they use through our single network.

Our network

We've worked hard to build a network like no other in Africa. One that benefits all of our customers, from the biggest corporate to the man on the street. Liquid Telecom has built Africa's largest independent fibre network which runs from the north of Uganda to Cape Town, covering Africa's fastest-growing economies, where no fixed network has ever existed before.



AFRICAN OFFICES

MAURITIUS (Head Office)
5th Floor, Ebene Mews 57 Cybercity
Ebene
Tel: +230 466 7620 Fax: +230 467 8263

BOTSWANA
F20, 1st Floor, Fairground Mall
Samora Machel Drive Gaborone
Tel: +267 391 8533
Fax: +267 391 8531

DRC
Boulevard du 30 Juin Immeuble Ruwenzori
5eme Niveau Local A Kinshasa/Gombe
Tel: +243 816 515 039

KENYA
Sameer Business Park Block A
Mombasa Road Nairobi
Tel: +254 20 5000 000
Fax: +254 20 5000 329

LESOTHO
Kingsway Street
PO Box 1037
Maseru 100
Tel: +266 22 21 1000
Fax: +266 22 21 1178

RWANDA
Avenue De L'Armee KN 67 ST #3
P.O.Box 6098 Kigali
Tel: +250 252 503 571

SOUTH AFRICA
150 Bryanston Drive Bryanston 2196
Johannesburg
Tel: +27 10 120 0400

UGANDA
Plot 26, Wampewo Avenue Bakwanye House,
PO Box 8373 Kampala
Tel: +256 20 240 1100 / +256 41 456 2800
Fax: +256 41 434 2192

ZAMBIA
Elunda 2
Addis Ababa Roundabout
Rhodes Park
Lusaka
Tel: +260 211 374 60 / 260 211 374 605
Fax: +260 211 374 622

HAI ZAMBIA
Pangea Office Park
Office Number 2,
Arcades Off,
Great East Road Lusaka
Tel: +260 211 255 037
+260 211 255 038

ZIMBABWE
4th & 5th Floors,
ZB Life Towers
77 Jason Moyo Avenue
Harare
Tel: +263 8677 030 000

ZOL ZIMBABWE
3rd Floor Greenbridge Eastgate
Cnr R Mugabe / Sam Mujoma Street Harare
Tel : +263 8677 177 177

REST OF THE WORLD

UNITED KINGDOM
6 New Street Square
London EC4A 3BF
Tel: +44 20 7101 6100 / +44 20 7101 6200

UNITED ARAB EMIRATES
Dubai Distribution Centre RA08FH01
Jebel Ali Freezone North (JAFZA)
Dubai, United Arab Emirates
Tel: +971 042 865 866

LIQUID TELECOM