Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 5 >>> MAY 2015

The Growing Threat of Cyber Attacks in Africa

By Timothy Harkness, Anupreet Amole and Emily Holland, of Freshfields Bruckhaus Deringer LLP.

You wouldn't buy a house in a crime-ridden neighborhood and not fit locks on the doors, or publish your bank details on a website where they could be seen by anyone who cared to look. But that's in effect what some of the world's biggest businesses are doing by failing to address cybersecurity standards in Africa. The highest-profile attacks may happen in the West, but multinationals are potentially more vulnerable in other territories.

The continent of Africa has become the El Dorado of espionage, according to a serving foreign intelligence officer recently interviewed by The Guardian.[1] The statement followed a leak of South African security files to Al Jazeera revealing the extent of spying activity within its borders. The U.S., the U.K., India, and Senegal are all reported to have dispatched agents to the country. Why are they there? In search of information about terrorist groups, defense systems — and businesses. Economic and technological theft were identified as among the principal reasons intelligence agents are focused upon the continent.

The New Scramble for Africa

Trillions of dollars have poured into Africa in recent years. The most recent African Economic Outlook report from the African Development Bank, the United Nations, and the Organization for Economic Cooperation and Development predicted that foreign investment on the continent would hit a record U.S.$84.3 billion last year. China has long been among the largest overseas investors, and in 2009 overtook the U.S. as Africa's biggest business partner. Other states including Singapore and Japan are becoming increasingly active, spending huge sums on energy and infrastructure assets, and to establish new markets for domestic products.

While investment has given foreign powers greater influence in Africa, not all activity has been overt and transparent. The Al Jazeera cables allege that China broke into South Africa's main atomic research facility in an attempt to steal information on the country's pebble bed nuclear reactor, and Beijing is surely not alone.

If nation states are using espionage to advance their interests, and those interests are increasingly commercial, then it's safe to assume that corporations will also be in their sights. Both Iran and Russia have been implicated in cyber attacks on major corporations, and they have in turn accused their rivals of doing likewise. At a recent cybersecurity briefing for retailers at Freshfields' London offices, a U.K. government spokesman warned delegates they should be alive to the threat from nation states that are "incredibly interested" in their mergers and acquisitions activity.

Technological Development Brings Opportunities — And Threats

Why are cyber attacks a growing threat in Africa? Much of the investment in infrastructure has been used to build communications networks. Internet, mobile, and

smartphone penetration is growing, with Cisco predicting there will be 598 million smart devices in Africa by 2018, up from 133 million two years ago. Cloud traffic is expected to increase by over 800 percent between 2012 and 2017.

This explosion in Internet access will further fuel economic growth and create a new wave of African startups. Already Nigeria is emerging as a technology hub, with venture capital pouring into a string of tech businesses. IBM has launched innovation centers in Kenya, Morocco, Nigeria, and South Africa, while Samsung has established "digital villages" (which aim to use technology to "positively impact the lives of five million people by the end of 2015") in Gabon, Congo, Ghana, Nigeria, Tanzania, and Sudan, and with more on the way in Ethiopia, Kenya, and Zimbabwe. Google, Facebook, Wikipedia, and France's Orange are vying for Internet users across Africa, entering into deals with service providers and offering users freebies. And Microsoft's 4Afrika and Biz4Afrika initiatives are designed to boost innovation and foster economic development across the continent.

We know from our own research that African assets are already attracting the world's biggest financial investors.[2] Deals by private equity firms in 2013 made up a greater proportion of total African M&A activity than ever before. And the largest global funds are becoming more active on the continent, investing over twice as much in the first half of 2014 as they did in the same period the previous year.

Corporate activity is also on the rise, with SABMiller and Coca-Cola merging their bottling concerns in southern and eastern Africa to create a U.S.$2.9 billion business, and Qatar National Bank investing U.S.$500 million in the pan-African lender Ecobank. Investors are seeing the same potential in Africa that has attracted China and other nation states — natural riches and an expanding middle class. Africa's technological evolution will rapidly expand potential markets — McKinsey predicts African e-commerce revenues will hit U.S.$75 billion by 2025 — and create assets whose value will be linked to the data they hold.

But unless Africa's cybersecurity infrastructure takes a massive step forward, acquiring them will require extremely careful risk management.

Cyber Attacks Put Deals at Risk

Cybersecurity is still woefully underestimated as a risk factor in the M&A process. In a July 2014 Freshfields survey of more than 200 global dealmakers, 78 percent of respondents said that cybersecurity was not analyzed in great depth or specifically quantified as part of the typical M&A due diligence process.[3] This despite 83 percent saying that a deal could be abandoned if previous cyber breaches were identified — and 90 percent saying such breaches could reduce the value of the target. The number of cyber attacks is rising despite a greater focus on information security, particularly in Europe and the U.S. Major corporations including Target, Sony, and JPMorgan have fallen victim to cyber incidents in recent months. If this level of complacency exists despite such high-profile attacks, then it's surely only a matter of time before a major multinational's subsidiary, office, or operation is compromised in Africa.

Cyber breaches raise a variety of risks for businesses, from regulatory (market disclosure obligations) to contractual (potential breach of confidentiality agreements with counterparties), monetary (a pending EU data protection regulation threatens fines of between 2 percent and 5 percent of global revenues for violations), and reputational. While sanctions and anti-bribery are rightly scrutinized during African transactions, cybersecurity should also be analyzed. We've been told nation states are keen to gain access to intelligence on M&A activity. If businesses in relatively well-protected countries are being warned by their own governments to be wary of such attacks — and are considering acquiring African assets — the weakest link in the chain is surely a logical point of attack.

If cyber criminals can thwart the best efforts of Western governments and corporations, then doing business in Africa presents particular risks. There are insufficient laws and regulations across the continent that recognize the pervasiveness of cybercrime and prescribe clear penalties for offenders. The cyber skills of law enforcement agencies, governments, and private sector organizations are low, while security controls at the personal, institutional, sectoral, and national levels are largely absent. There are also few national databases to track criminals — perhaps explaining why 3 percent of all malicious apps and programs are reported to originate in Nigeria. There's still a huge amount to be done to boost security in the U.S. and Europe — and Africa is already years behind.

The Corruption Challenge

Good cyber governance is about more than just technology. It's about managing behavioral risk, as Edward Snowden and Chelsea Manning, reports from professional services networks and cybersecurity firms, and massive breaches such as Target and Morgan Stanley, highlighting the threat from within (employees and vendors), have shown.[4] Tackling this in Africa is a monumental challenge. The continent is prone to corruption, providing 15 of the 30 worst offending countries in Transparency International's 2014 Corruption Perceptions Index. Other aspects of the behavioral problem are illustrated by one of the classified files passed to Al Jazeera — a South African intelligence report entitled "Security Vulnerabilities in Government." The file lists laptop thefts, unencrypted communications, and limited vetting of senior officials as some of the reasons why the government is so vulnerable to spying. With valuable data at stake, businesses should also guard against internal dangers.

Africa accounts for 2 percent of global gross domestic product but suffers 10 percent of global cybercrime incidents, with Kenya, Nigeria, and South Africa identified as growing hubs of criminal activity. Our recent study revealed that the latter countries are the two most attractive to private equity investors. Yet data from Symantec

   ISSN 1473-3579

reveals that only Russia and China have more victims of cybercrime each year than South Africa. Cyber attacks cost the country R5.8 billion (approximately U.S.$481 million) every year,[5] with recent strikes on institutions including Gautrain Management Agency, Postbank, the governing African National Congress, and even the country's police service. On average, cyber attacks on South African organizations go unnoticed for 200 days.

The situation in Nigeria is similar. Data breaches rose by 62 percent in 2013, and both Deloitte and Cisco have warned the country it is at risk of a major attack. In January, the website of Nigeria's Defense Headquarters was compromised in an "ISIS-style attempt" to hack into government platforms. Cisco singled out Nigeria's banks, oil and gas companies, and government as being particularly vulnerable.

Criminals Target Valuable Data

The industries most attractive to foreign investors are also those that face the biggest cyber threat. Retail and telecommunications companies hold large quantities of personal data. Africa's banks are rapidly transitioning their customers to mobile platforms, raising their cyber risk profile. There is evidence that alongside industrial espionage, energy businesses are prone to cyber attacks during M&A transactions, particularly when foreign investors are competing against state-owned enterprises.

While moves have been made to tackle the threat, the response has been patchy. Cybercrime-related laws are beginning to emerge but there is an urgent need for these to be clarified, strengthened and harmonized across borders. There is anecdotal evidence that existing legislation is incoherent and poorly understood.

Several countries are adopting or are expected to adopt national cybersecurity strategies (including Kenya, Nigeria, South Africa, and Uganda). Others are developing cybercrime coordination centers, with central African governments recently announcing a plan to pool their resources. Some countries have instituted data protection laws and established data protection regulators. But even here there are major gaps around investigative measures, jurisdiction, and how to collect electronic evidence. And without the skills to investigate cybercrime, no amount of legislation will be enough.

Transnational bodies are trying to tackle the issue, including the UN (via its African Center for Cyber Law and Cybercrime Prevention) and the Commonwealth (which has launched its own Cyber Initiative). The U.S. government's "cyber diplomacy" strategy encourages countries to adopt the Budapest Convention, which includes strong, harmonious cybercrime laws and a comprehensive set of investigative tools to address high-tech crime and conduct digital forensics. It is also trying to build technical skills by engaging with governments and local law enforcement agencies and running training programs across the continent.

Action is Needed — And Not Just from Governments

Alongside this Africa is pursuing its own agenda, with the African Union passing its Convention on Cyber Security and Personal Data Protection at a recent summit (*see analysis at WDPR, August 2014, page 21*). The Convention — based on the EU's framework — covers online activities including e-commerce, data protection, and cybercrime, and would see nations enact personal data protection laws upheld by new public authorities. But implementation of the Convention is a long way off. The Convention must be signed by 15 countries to enter into force, and after that national implementing laws would need to be passed. No country has yet ratified the Convention.

The solution to Africa's cyber challenges will not come from governments alone. Businesses must set up cross-functional teams to review their current practices, policies, and procedures, and implement a crisis response plan in tandem with their external advisers, including lawyers. Businesses must address the technical and behavioral risks associated with cyber attacks and must review their data gathering, use, and retention procedures. And they must beef up their information security around transactions and disputes, particularly investor-state arbitrations.

The digital revolution has the power to transform Africa. But unless cybersecurity standards improve, that potential could be squandered.

If Africa is a new El Dorado, then those seeking to do business there should secure their information assets before it's too late.

NOTES

[1] http://www.theguardian.com/world/2015/feb/24/africa-el-dorado-espionage-leaked-intelligence-files.

[2] http://www.freshfields.com/uploadedFiles/SiteWide/News_Room/News_/01795_MKT_WWW_PE_Growth_In_Africa_INTERACTIVE_AW.PDF.

[3] http://www.freshfields.com/uploadedFiles/SiteWide/News_Room/Insight/Campaigns/Cyber_security_in_MandA/01214_BS_MBD_Media_MA%20Cyber%20Security%20Report_WEB_AW.PDF.

[4] http://www.pwc.com/crimesurvey; http://www.kpmg.com/SG/en/IssuesAndInsights/ArticlesPublications/Documents/Advisory-CS-Data-Loss-Barometer.pdf; http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/; http://www.wsj.com/articles/puzzle-forms-in-morgan-stanley-data-breach-1420590326.

[5] http://www.itwebafrica.com/security/514-south-africa/234242-cybercrime-costs-sa-economy-r58-billion-annually.

Timothy Harkness is a Litigation Partner based in Freshfields' New York office and may be contacted at timothy.harkness@freshfields.com. Anupreet Amole is a Senior Associate in Freshfields' Commercial Litigations Group based in the firm's London office and may be contacted at anupreet.amole@freshfields.com. Emily Holland is an Associate based in Freshfields' Washington office and may be contacted at emily.holland@freshfields.com.