e-Zine

INFORMATION BULLETIN OF THE ACP BUSINESS CLIMATE FACILITY

BizClim

September 2012 / N13

Table of contents

The importance of cyber security in business

Speaking at the Africa Forum on Cyber Security in Nairobi, Kenya, on September 13th-14th, M'Hamed CHERIF, Director of BizClim, pressed the need to integrate cyber security into the business and investment climate agenda and to follow a coordinated approach.

Whilst indicators, rankings and benchmarking studies abound, covering almost every important aspect of the business climate, information on cyber security is rather scant and has not yet been mainstreamed in business climate analysis. Only one cyber security index is available for the United States, which measures changes in perceptions.

In African countries where studies have been undertaken, the vulnerability to cyber crimes seem to be alarming. Some countries such as South Africa, Nigeria and Ghana rank high on crime in the IC3's Internet Crime Report. According to a recent survey by Deloitte, 60% of banks in East Africa are susceptible to security threats because of low IT budgets. In Kenya alone, the Central Bank estimates that local banks lose $2.8 million to fraud annually. Early this year in South Africa, hackers snatched $6.7 million from Postbank in approximately 72 hours. Cyber crime activities range from purely malicious or intimidatory invasions of privacy to theft. At the level of state security, instances of data destruction through electronically-transmitted malicious software have been reported. A common thread connecting these activities is the intrusive abuse of computers. Information-stealing malicious software (malware) has become quite common, but is not generally known to smart phone users. Security can at times seem like an overwhelmingly complex challenge. Threats to data, both real and perceived, loom from all angles. Hacker attacks, disgruntled or dishonest employees, and competitive snooping are just some of the concerns with respect to the protection of proprietary information.

Vers un environnement favorisant le développement du secteur privé

Une Facilité financée par l'Union Européenne par le biais du Fonds Européen de Développement (FED)

The ACP Business Climate Facility (BizClim) provides technical assistance that is essentially about improving regulations, legislation, the institutional set up and financial measures (the rules of the game) relating to the enabling environment of the private sector in ACP countries or regions and to do so by focusing on possible support to ACP governments or regional institutions and private sector organizations.

Responsible Editor
M'Hamed Cherif
Rue Belliard, 205
1040 Brussels - Belgium
Tel: +32 2 669 98 25
Fax: +32 2 669 97 86
info@acpbusinessclimate.org
www.acpbusinessclimate.org

Cybercrimes: insidious and with a huge impact

Concerns are already being voiced about the negative effect that cyber crimes can have on investment, notably in the ICT sector and beyond. The failure to fully integrate these concerns into trade and investment debates is likely due to uncertainty about the full range of cyber crimes and how they affect daily life, but these threats are real and far-reaching. Targeted attacks, which increased dramatically in 2011, affect all sectors of the economy and could even be used to cause physical damage in the real world, materializing the spectre of cyber-sabotage. Advanced persistent threats (APTs), which have become a buzzword, aim at obtaining highly-valuable information and stealing intellectual property.

African governments pushed to take actionr

Both businesses and governments are now pushed to take action to protect their citizens and to ensure the security of sensitive information. Undoubtedly, a lack of appropriate guidelines and relevant laws has led to some criminals going unpunished. Some African governments have recently set up incident reporting and early warning bodies with the support of AfriNIC (Africa Network Information Center). For example, South Africa, Kenya, Morocco, Ivory Coast and Tunisia have set up Computer Emergency Response Teams (CERT) that will work with information security professionals to report vulnerabilities and detect DDoS (distributed denial-of-service) attacks. The move is coordinated by AfricaCERT.

Several African countries have begun enacting cyber security standards aimed at curbing Internet insecurity. The move follows a spate of hackings of a number of websites owned by African governments, which points to weak ICT security systems and regulations on the continent. In Nigeria, a Cyber security bill will soon be passed into law, helping the country to enhance its image online and globally. The Government of Ghana is setting up an emergency Cyber Crime Response Team, to review existing legislature governing Information Communication and Technology (ICT) activities and to strengthen the country's cyber security.

Faced with a long and growing list of international regulations affecting IT security, compliance is viewed as one of the top concerns for many private sector executives. Some of these laws hold organisations accountable for protecting the confidentiality of consumer or patient information. Others require companies to provide detailed and reliable documentation on financial decisions, transactions and risk assessments. New laws are being passed all the time.

In the fight against cyber crimes, African countries are obliged to enhance coordination and cooperation between themselves and the rest of the world. In this regard, the United Nations African Institute for the Prevention of Crime and Treatment of Offenders (UNAFRI) launched the African Centre for Cyber Law and Cybercrime Prevention (ACCP) in Kampala, Uganda in August 2010, in response to the growth of mobile phone banking. The approach of West African countries, based on a common regional anti money-laundering legislation, is the way forward in addressing the threat of cyber crime. ■

Selected BizClim Events

Titre	Beneficiary	Place and Date
Enhancing financial services in the Eastern Caribbean	ECIC Holdings Limited	St Kitts, 10th-11th September 2012
Building business value supply chain in the Pacific region	PIPSO	Fiji, 11th-12th October 2012
Enhancing African Investment Promotion Agencies' websites and marketing tools according to global investment promotion benchmarking reports	COMESA RIA	Seychelles, Democratic Republic of Congo, Malawi, Uganda, 22th October 2012

Threat grows faster than prevention

Whilst news on violent crimes frequently hit the national and international headlines, the less-reported occurrence of cybercrimes is on the rise. In 2011, Symantec blocked more than 5.5 billion of malicious Internet attacks. Increased use of mobile phones and faster access to social media and the internet can partly explain the increase in cybercrimes and escalation of risks, with increased chances for interception of valuable data.

Mobile and online banking are the fastest-growing online services, and criminals are quickly adapting too. According to Symantec, 2011 was the first year that mobile malware presented a tangible threat to enterprises and consumers.

The Global Cybersecurity Agenda estimated that in 2010, cybercrime was responsible for more than US$105 billion of online property losses worldwide. In 2011, hackers made off with 1.5 million records from an electronic payments processor in what has been called the RBS Worldpay Scam. The scam involved the production of made fake ATM cards, which were used to withdraw more than $9 million in 49 cities around the world in a one-hour period.

A dragnet in the U.S. and the U.K. brought in a sophisticated international criminal gang attacking small business bank accounts in October 2010. Authorities arrested more than 60 people connected with an Eastern European information theft ring. Indictments charged gang members with using the Zeus Trojan to steal more than $3 million from online corporate financial accounts. Over the years, cyber criminals have targeted data storage cards to 'harvest' financial account information. In South Africa, for example, knowledgeable runners instruct waiters or waitresses to collect data from credit and debit cards using portable scanners. The collected data is subsequently transferred to cloned-cards for use in commercial transactions or for fund withdrawals.

Today, small businesses around the globe are squeezed between extremely tight IT budgets and ever-increasing national and international requirements to protect sensitive information. Security and compliance can seem like impossible tasks. ■