Measuring Information Security: Understanding And Selecting Appropriate Metrics

Perpetus Jacques Houngbo *jacques.houngbo@imsp-uac.org*
Institut de Mathématiques et de Sciences Physiques (IMSP)
Dangbo, Benin

Joël Toyigbé Hounsou *joelhoun@gmail.com*
Institut de Mathématiques et de Sciences Physiques (IMSP)
Dangbo, Benin

Abstract

Thanks to numerous information in newspapers about data leaks, advocacy for information security is no more that difficult. But on the practical side, it is usually tough time for information security professionals when they have to demonstrate the value of information security to their organizations; they have so much metrics available on hand that making the right selection is far from obvious. This paper is about understanding the metrics that are available and discussing how to use them in some specific less developed economies.

Keywords: Information Quality, Measurement, Metric, Performance.

1. INTRODUCTION

The spate of attacks against information assets, as reported by media, leads to the fact that it is more or less widely accepted that information security is important. The 2014 *Cost of Cyber Crime Study: United States* report published by the Ponemon Institute indicates an average number of 1.7 successful attacks per company each week[1]. That number is a clear increase from the 1.3 successful attacks per company each week observed in 2012. While analyzing the security breaches, PwC[2] notices that "7% of the worst security breaches were partly caused by senior management giving insufficient priority to security (down from 12% a year ago)". Thanks then to those numerous information disclosed in newspapers about data leaks, advocacy for information security is no more that difficult. It is no more only IT professionals who care about information security. Top management and even boards pay attention to the issue [3].

At least, that is the situation in developed countries.

But other parts of the world are also improving their commitment to information security.

During its 23rd ordinary session held in Malabo from 26 - 27 June 2014, the African Union has adopted as a legal instrument a "Convention on Cyberspace Security and Protection of Personal Data" [4].

That instrument is expected to lead to the definitions on key cyber terminologies in legislation and to harmonized cyber legislation and provisions for the African Union. The instrument has still long way to go, but at least, awareness and concern about cybersecurity is moving to top in the mind of leaders.

This paper is about recall of the rationale of measuring information security; it is about tools for better understanding and better control on information security. The next section, section 2, will cover the answer to the question of measuring information security and will present a literature summary of what measurement is. In linking to the specific field of information security, there will be an overview of how to measure, what is to be measured. The section 3 is an overview of the

collection of metrics; it will present types of metrics and their classification. The discussion part in section 4 is about the differentiation between enterprise level and national level and will also link to less developed economies.

This paper doesn't pretend to be comprehensive: its purpose is to join the discussion and to contribute with reflexion on some specific needs in the African Continent.

2. UNDERSTANDING METRICS

2.1 Why Measuring Information Security

Usually, when available, cyberstrategies state visions to protect economies. At the level of transformation of that vision of improving information security into facts, at the point of implementation of those wills, there are many solutions, many options. And the permanent question is to know to what extend all initiatives are pertaining, are effective, are efficient. It is about knowing and being able to demonstrate that the actions have lead from a level B of information security to a level C or D, which is supposed to be better.

Measuring information security using consistent metrics improves ability to understand it and control it.

What comes automatically to mind at this point is the well known say from the international performance improvement and quality guru H. James Harrington. "*Measurement is the first step that leads to control and eventually improvement. If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it.*" http://www.goodreads.com/author/quotes/42617.H_James_Harrington[1].

That is the reason why numbers are used to illuminate an organization's security activities [5]. Information security metrics offer opportunity to identify sources of security data, to assert the pertinence of security data in alignment with the business, to associate numbers to activities that have been traditionally hard to measure.

2.2 What is a Metric

Understanding the different metrics available for information security starts with a recall of what a metric is.

The Oxford online dictionary defines metric as a system or standard of measurement. And it defines measurement as the action of measuring something, the action of ascertaining the size, amount, or degree of (something) by using an instrument or device marked in standard units[2] [3] [4].

Metrics and measurement are intimately linked. Although they are often used one in place of the other, they are different. In the rest of this paper, the option has been made to use them

---

[1] Previous versions of that quote are due to Lord Kelvin."To measure is to know."

"If you can not measure it, you can not improve it."

"In physical science the first essential step in the direction of learning any subject is to find principles of numerical reckoning and practicable methods for measuring some quality connected with it. I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science, whatever the matter may be." [PLA, vol. 1, "Electrical Units of Measurement", 1883-05-03]

Some may notes that H. James Harrington added the concept of control.

[2] http://www.oxforddictionaries.com/definition/english/metric

[3] http://www.oxforddictionaries.com/definition/english/measurement

[4] http://www.oxforddictionaries.com/definition/english/measure

interchangeably, in adoption of a posture similar to the one of Applied Computer Security Associates (ACSA) [6], as will be explained in the coming paragraphs.

Metric is usually presented as an abstract, a subjective attribute [7], while a measure is a concrete, objective attribute. Measurement results from an observation, using some appropriate method to collect data and metric represents the observed data in kind of scale [8]. After making observations to realize measurements, analysis is performed to generate metrics [9].

Some authors have specifically defined what a good security metric should be. This makes the assumption that security is measurable.

2.3 Is Security Measurable

Wondering if security is measurable is a genuine question.

Like attributes such as beauty, scent, or flavor, or factors such as motivation and intent, security is intangible. Security offers then very fews mean to operate any direct measurement. Security is an abstraction, a concept, an idea, a notion, as opposed to a fact or a material consideration.

So far, measuring intangible happens very often. Teachers are measuring their student knowledge when they grade them, managers are measuring their staff performances when they grade them, IT professionals measure “strategic alignment”, “customer satisfaction”, “employee empowerment” or “improved performance” as benefits of IT projects when presenting them for decision of top management. Douglas Hubbard [10] is even stating that “everything is measurable”. When he says that he hasn’t *found a real ‘immeasurable’ yet*, he has developed, among many, measure of the risks of cyber attacks.

Because intangibles are mostly based on attitudes and perceptions, they are often measured qualitatively in terms of “disagree or agree” on an X-points scale.

Coming back to information security, the real need for measurements derives from the imperious necessity for managers to have tools that can assist in giving answers to fundamental questions and concerns like[11] : (i) Is my organization secure? (ii) Are the personnel sufficiently educated and trained to minimize the risks to the organization? (iii) Is my organization complying with regulations on managing and safeguarding sensitive data? (iv) How do I measure the security risk of a new technology or service provided to our customers? The main measurement objective[12] is the correctness of the different security controls that will then be enforced.

A broader answer to the reason why such intangible like information security should be measured is provided Karl-Erik Sveiby[13]. Motives of measuring are [should be]: control (to monitor performance), valuation (to acquire/sell business), justification (to report to stakeholders), decision (to guide investment), learning (to uncover hidden value).

In using the terms metric and measurement in relation to information security, there are many controversies; they range from scientific principles to results of assessments based on subjective judgments, from dictionary or scientific definition to actual usage adopted in policies and practices [6].

The Applied Computer Security Associates (ACSA) has been well inspired by deciding to use the expression *information security (IS)**, the asterisk (*) meaning any of the following terms: metric, measure, score, rating, rank, or assessment result, etc. That decision reflects the actual usage of the terms, even if many admit the misuse of them. The Applied Computer Security Associates (ACSA) has then defined IS* *as a value, selected from a partially ordered set by some assessment process, that represents an IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence* [6]

2.4 Defining Good Security Metrics

As we are moving on with information security being measurable, what will the good metrics for

that purpose?

Many authors have suggested different ways of appreciating a good metric. John Wesner and Georges Jelen are among those who first applied the definition of “smart” to information security metrics. According to them, a good metric is s m a r t:

- specific: clear in what it is measuring, well defined, using unambiguous language;
- measurable: with a quantitative definition;
- attainable: is in the reach, is within budgetary and technical limitations of those in charge of measuring it, is right up their alley;
- repeatable: record the same value, the same measurement when different measurement takers look at the same phenomenon;
- time-dependent: with measurements only valid for finite periods of time.

Barabanov et al.[14] has listed some other examples of proposed definitions of ideal security metric characteristics:

- accurate, precise, valid, and correct (Herrmann, 2007);
- meaningful, reproducible, objective and unbiased, and able to measure progression towards a goal (Chapin & Akridge, 2005);
- consistently measured, cheap to gather, expressed as a cardinal number or percentage and using at least one unit of measure, and contextually specific (Jaquith, 2007).

Some recent works [15] recommend to use PRAGMATIC security metrics. Pragmatic metrics have:

- predictiveness: helping to know what is likely to happen, before it happens, in good time to do something about it;
- relevance: aligning information security to the business of the organization;
- actionability: acting like course beacons, telling in which direction and to what ex- tend to adjust the course;
- genuineness: reducing [eliminating] biases and opportunities of game-playing;
- meaningfulness: telling clear story to the audience, who can then act immediately and with full knowledge of the facts;
- accuracy: presenting precision;
- timeliness: being available when the right persons can act on it;
- independence: possibility of verification by trustworthy, impartial party;
- cost-effectiveness: demonstrating clear benefits to the business of the organization.

One can think that “common sense” approach has guided many of the previous and this is beneficial as “common sense” usually contains “*good sense and sound judgment in practical matters*”.

3. TYPE OF METRICS

3.1 Standardization Efforts

Mainly started from within the USA digital economy, there are initiatives to establish standardized enumerations. Objective is to develop and adopt common standard languages and concepts for

organizations around the world to be able to share information and measurement goals. The MITRE Corporation[5] and the NIST (National Institute of Standards and Technology)[6] are very active on those standardization efforts, and they are quite well seconded by CERTs and CSIRTs, by organizations likes FIRST (Forum for Incident Response and Security Teams)[7]. The ITU-T, Study Groups of ITU's Telecommunication Standardization Sector which assemble experts from around the world to develop international standards known as ITU-T Recommendations, has for instance passed a recommendation on the use of the common vulnerabilities and exposures (CVE), the recommendation ITU-T X.1520 (01/2014) [16].

The standardization efforts are mainly grouped into three blocks: enumerations, languages, repositories.

Robert A. Martin [17] explains that enumerations catalog the fundamental entities and concepts in information assurance, cybersecurity, and software assurance that need to be shared across the different disciplines and functions of these practice. They focus on quantification, ranking, and evaluation of cybersecurity and information assurance. The enumerations are basically useful for identification of weaknesses or vulnerabilities based on severity and impact, classifying and prioritizing them. They also enable selecting appropriate remediation for those vulnerabilities.

The following table lists some enumerations.

Name	Description
Common Vulnerabilities and Exposures (CVE) http://cve.mitre.org/cve/	Standard identifiers for publicly known vulnerabilities
Common Weakness Enumeration (CWE) http://cwe.mitre.org/data/	Standard identifiers for the software weakness types in architecture, design or implementation that lead to vulnerabilities
Common Attack Pattern Enumeration and Classification (CAPEC) http://capec.mitre.org/data/	List of common attack patterns, includes comprehensive schema and classification taxonomy
Common Configuration Enumeration (CCE) http://nvd.nist.gov/cce/index.cfm	Standard identifiers for configuration issues
Common Platform Enumeration (CPE) http://nvd.nist.gov/cce/index.cfm	Standard identifiers for platforms, operating systems, and application packages

TABLE 1: Sample of Enumerations.

[5]http://www.mitre.org/
[6]http://www.nist.gov/
[7]http://www.first.org/global/standardisation/cybex/structured.html

The next block of tools in the architecture of standardization initiatives are languages: they are interface standards for conveying high-fidelity information shared among humans, tools and organizations.

The following table lists some languages.

Name	Description
STIX (Structured Language for Cyber Threat Intelligence Information) http://stix.mitre.org/	Collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information
TAXII (Trusted Automated eXchange of Indicator Information) http://taxii.mitre.org/	Set of services and message exchanges that enable sharing of actionable cyber threat information across organization and product/service boundaries
OpenIOC (Open Indicators of Compromise) http://openioc.org/	Extensible XML schema for the description of technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise
Extensible Configuration Checklist Description Format (XCCDF) http://scap.nist.gov/specifications/xccdf/	Information Assurance Vulnerability Alerts (IAVAs) and Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGS)
The Center for Internet Security (CIS) http://www.cisecurity.org/	CIS Security Configuration Benchmarks
National Security Agency (NSA) https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/	NSA Security Guides
OVAL Repository http://oval.mitre.org/repository/	OVAL Vulnerability, Compliance, Inventory, and Patch Definitions

TABLE 2: Sample of Languages.

The other block that contributes to standardization is about repositories. They point to where standardized content are made available for sharing.

The following table lists some repositories.

Name	Description
Center for Internet Security (CIS) Consensus Security Metrics Definitions http://benchmarks.cisecurity.org/downloads/metrics/	Set of Consensus Security Metrics and data set definitions that can be used across organizations to collect and analyze data on security outcomes and process performance
Red Hat OVAL Repository https://www.redhat.com/security/data/oval/	OVAL definitions for Red Hat Enterprise Linux 3 and above
Debian OVAL Repository http://www.debian.org/security/oval/	Debian OVAL Repository
IT Security Database OVAL Repository http://www.itsecdb.com/oval/	OVAL(Open Vulnerability and Assessment Language) definitions from several sources like Mitre, Red Hat, Suse, NVD, Apache etc

TABLE 3: Sample of Repositories.

The previous paragraphs have presented excerpt of the standardization initiatives, some- times cross-referenced. They have proven to be very effective in enabling security operations measurement and policy compliance efforts.

The classification effort of security metrics continues with the following categories.

3.2 Diverse Classifications of Security Metrics

The CIS, Center for Internet Security

The CIS, Center for Internet Security [18], has defined a set of security metrics that can be grouped in management metrics, operational metrics or technical metrics based on their purpose and audience.

Category	Scope
Management metrics	Provide information on the performance of business functions, and the impact on the organization Audience: Business management
Operational metrics	Used to understand and optimize the activities of business functions Audience: Security management
Technical metrics	Provide technical details as well as a foundation for other metrics Audience: Security operations

TABLE 4: The CIS Security Metrics.

Metrics in the view of business imperatives for information security

After analyzing the determinants of the business imperatives for information security, Gary Hinson and Krag Brotby [15] have made a kind of update to the list in the previous paragraph. The determinants are the organization's purpose, objectives, business strategies, risks and opportunities and what the organization wants to achieve through information security. This will lead to the definition of the security metric that are needed. For the sake of that selection, metrics have been grouped in three categories:

Name	Description
Strategic security metrics	Measures concerning the information security elements of high level business goals, objectives and strategies.
Security management metrics	Metrics that directly relate to achieving specific business objectives for information security
Operational security metrics	Metrics of direct concern to people managing and performing security activities: technical and nontechnical security metrics updated on a weekly, daily or hourly basis

TABLE 5: Types of Security Metrics.

Metrics supporting control objectives

The information security business has designed many security frameworks that are internationally used. Among the most popular are the *Control Objectives for Information Technology (COBIT)*, the *ISO 27000 series of standards, specifically designed for information security matters* and the *Information Technology Infrastructure Library (ITIL)*.

Professionals also often refer to the set of documents about information security that the United States National Institute of Standards and Technology (US NIST) publish under the Special Publication 800 Series. Those frameworks enumerate some metrics that are tightly connected to the control objectives of the frameworks. The control objectives covered [19] are:

- information security policy document
- review of the information security policy
- inventory of assets
- ownership of assets
- acceptable use of assets.

With those various security metrics in hand, IT professionals can rely on scorecard to assist in using the metrics outside the IT room. A scorecard is a *statistical record used to measure achievement or progress toward a particular goal*. Such tools are very valuable when aligning some function to the business, as is the case of information security. A security scorecard connects the organization's strategies and policies in information security to their potential to improve the core business.

The security scorecard is an effective internal communication tool for organizations. Numerous benefits are attached to a security scorecard. Tightening security program to business improves implementation of that program as there is no more discussion about what are the values it adds to the business. The process of request for resources is softened and credibility of the request as well as the one of the program are increased. This goes with increase in accountability: those allocating resources know exactly what they are allocating them for and those in charge of implementation[20] of the program have clear view of what results they accountable for.

Establishment of a security metrics program or design of a security scorecard is a matter of appropriate combination of several ingredients that are expected, once mixed together, to produce the unique product that will serve the organization. Most authors, [9], [21] and [15] for example, insist on the starting point being the organization's purpose. The organization's objectives indicate why information security can be relevant to the business executives. And the answer to that question is selecting which metrics have to be present in the security scorecard. The metrics integrated in security scorecard convey appropriate information and message to the executive but before having them, the IT team may need to elaborate metrics at another granularity level, such as security metrics from network attack graphs [21] [22] [23].

4. DISCUSSION

From the previous sections, one can say that there is no scarcity in security metrics. The challenge is to find one's way, to select those of the measurements that impact the business. This discussion will cover the difficulties in selecting the metrics that matter, the metrics that may pertain to special needs like those of small and medium enterprises (SMEs), the concerns of having indicators at national level, and the particular issue of less developed countries.

4.1 Difficulties in Designing A Security Metrics Program

Be they smart or pragmatic, security metrics included in a program have to be as good as defined previously in section2.4. This implies that the team in charge of the program must pay due attention to two important elements: selecting the measures and ensuring accuracy of measures.

Selecting the measures

In order to compute them and present them for decision, security metrics defined in security scorecard usually need to be translated in other "low level" security metrics. The numerous enterprise security controls commonly implemented in organizations can be source for this metrics. They include antivirus and anti spyware software, intrusion detection systems (IDSs), firewalls, patch management systems, and vulnerability scanners.

This profusion of data from the controls can lead to confusion and can overwhelm the team in charge of security metrics program. While most of them may be of high interest in the day to day operation of information security, not all of them can convey the necessary message to be included in the pool that will add value to the security scorecard. In other words, quantity is not necessarily the solution. The team has to select those few which can represent the broad figure. One solution among many is to evaluate the usefulness of those "low level" metrics and to design a plan for how to use them. This can save a lot of time and hassle.

Ensuring accuracy of measures

Accuracy of measures equate to their correctness, their precision. Basically, accuracy creates the conditions for confidence in the results of the measurements. This means that the measures have been defined precisely, with no room for misunderstanding and that the methods used for the measurements are consistent. It is advised to avoid qualitative measures that do not have well-defined scales or units of measure. They are too vulnerable to subjective variations.

Context is also very important to measures and metrics. Taken individually, metrics may convey only little meaning, but when put in their context and "correlated" to other, they can tell a useful and definitely different story. Hence, the need for analyzing single measures in context with other measures and even correlates them to events such as security control changes.

One of the guides published by the NIST is particularly useful in tackling those two groups of difficulties. Based on the NIST SP 800-53 Revision 4 Recommended Security Controls for Federal Information Systems and Organizations, the NIST Special Publication 800-55 Revision 1 [24] has listed 19 measures that can be analyzed for the implementation of an information security measurement program. It specifically insists on the factors to be considered:

- measures must yield quantifiable information (percentages, averages, and numbers);

- data that support the measures need to be readily obtainable;
- only repeatable information security processes should be considered for measurement;
- measures must be useful for tracking performance and directing resources.

The NIST Special Publication 800-55 Revision 1 specifies for every candidate measure the goal, the target, the formula, the type, the implementation evidence, the data source of collection, the frequency of collection and reporting, the responsible parties.

4.2 Security Metrics Program for a SME

All over along this paper, the importance of security metrics has been (re)stated for organizations, for private companies. This part of the discussion will now come to some specific private companies, aka to small and medium enterprises / small and medium industries (SMEs/SMIs) in Africa. While big firms are numerous on the continent, they are usually part of international groups, which are supposed or expected to be already applying all best practices in many management domains. The reality is more than probably different, but that aspect is intentionally set out of the scope of this paper. This paper wishes to focus on SMEs/SMIs.

On the African continent, SMEs/SMIs are known to be playing a pivotal role. The most common characteristics of Small and Medium Scale Enterprises (SMEs) as defined by[25] is that they are business *owned, led by one or a few persons, with direct owner(s) influence in decision making, and having a relatively small share of the market and relatively low capital requirement*. Such businesses are well known in the economic landscape of Africa. They represent 90% of privately-owned African companies, 33% of the continent's GDP and account for 45% of new jobs. To say it in the words of AfricSearch founder Didier Acouetey, *SMEs are vascularising the African economy* [26].

Where do SMEs stand vis-a-vis the concern of information security? The answer to that question is a key point before going to the level of appropriate metrics.

Kenya has designed a security framework for its SMEs[27]. But since "*the framework has not been tested in a real working environment of SMEs, further analysis on the effectiveness of the framework is required, and the results should be reflected in future frameworks*." [27]

There is an ongoing effort, among many other initiatives, to derive a better understanding of SMEs, in the economy of Republic of Benin for instance. Meanwhile, preliminary results show that the concerns of managers of SMEs are clearly far from information security. That situation is quite "understandable" for businesses that are suffering from overwhelming tax regimes, lack of services from governments (transport, energy, communication, shortcomings of the legal environment, etc.) and low access to financing. In such situation, information security can hardly come up in the priorities of managers and all the more security metrics in any scorecard.

In spite of the situation described above, it is important to find way to raise awareness of information security in the SMEs: 33% of the continent's GDP and account for 45% of new jobs are at stake, and more importantly, the whole "vascular system" of the African economy can be endangered. Being it for protecting [securing] their business or for growing their business, SMEs will benefit from alignment of information security to that business. This is part of ongoing work initiated in another framework.

4.3 Security Metrics Program for a Developing Country

The vast majority of security metrics has been defined for use at the level of organizations: private companies, governmental bodies, etc. But the concern of information security is also very present at the national level. Information security incidents on internet infrastructure tend to become daily occurrence. At first glance, statistics seem to be saying that less developed countries, especially those from the African continent, are not harmed by the phenomena of information security incidents. This may be due to the poor level of penetration of digital economy in the continent. On the other side, the lack of statistics usually reflects the poor monitoring and

fear of bad effect of disclosure of incidents. Meaning that information security incidents are more than certainly occurring, but very few are aware of them.

Some governments from less developed countries have decided to tackle the information security issue. They have designed policy pertaining to information security, they have published strategies, they have announced implementation plans. And then, the same type of questions at the level of organizations pop up for the national level. How secure is the country? How has the designed series of actions affected the security of the country? How do the country compare to other countries? What are the information security strengths and weaknesses? Etc.

Hence, the same need to have a security metrics program at the level of the country in order to assess the implementation of security capabilities, to measure their effectiveness, and to ascertain their impact on national economy.

There are many similarities in the cyberstrategies implemented by developed countries. After the establishment of its National Information Security Center (NISC), Japan for example has created an Action Plan on Information Security Measures for Critical Information Infrastructures. The current version, the third edition, clarifies the purpose of Critical Information Infrastructure Protection (CIIP) as follows [28]:

In order to continuously provide CII services and to avoid serious effects on the public welfare and socioeconomic activities from IT outages resulting from natural disasters, cyber-attacks or other causes, all stakeholders should protect CII by reducing the risk of IT outages as much as possible and by ensuring prompt recovery from IT outages.

Developed countries are globally complying with recommendations from industries [29], recommendations that can be grouped in the following categories:

- action plans to include the scope of critical infrastructure;
- information sharing with government organizations and system vendors, etc;
- cross - sector exercises for ensuring business continuity;
- platform for evaluation and authentication of such systems as control systems used by critical infrastructure, in compliance with international standards;
- common standards of information security measures for government agencies.

It is then obvious that important burdens still remain on the shoulders of government agencies, performance being measured at their level. Different key metrics [30] are then designed for those agencies and then monitoring for the nation is actually a meticulous process of collecting pertaining information from them [31].

Cybersecurity metrics at national level have then to be computed based on information compiled from the government agencies.

Developing countries seem to be hesitating [or reluctant] to enter that process. There are very few examples from the African continent, if any at all! It is common argument to pretend that scarcity of resources, both financial and human, hinder engagement in cyberstrategies. This misleading has to be corrected: today's economy is so tightly connected with information systems that information security must be understood as a "must have".

5. CONCLUSION

When talking about information security metrics, IT professionals have abundance of metrics at their hands for use. Developed countries are building best practices from cyberstrategies to monitoring of improvements of performances. Examples to follow and to improve are available, but less developed countries are not really engaging in that battle. The African continent has still long way to go: digital economy is improving but the pace of interconnection of the components of

the economy can be described as very low. SMEs as champion of the economic growth of the continent are seeing their business at risk with very little help from the governmental agencies in some countries. Those SMEs must find way to protect their information assets by aligning information security to their business and by design pertaining security metrics programs with metrics that must fit in their scorecards.

6. FUTURE RESEARCH

All over along this paper, some elements of future research have been clearly specified. Two of them are of importance and will be tackled in near future: information security for SMEs and performance monitoring of national cyberstrategies in the environment of less developed economies. The case of the economy of Benin will be the framework for applying the concepts presented above to the type of SME in place: a *business owned, led by one or a few persons, with direct owner(s) influence in decision making, and having a relatively small share of the market and relatively low capital requirement*.

7. REFERENCES

[1] P. Institute, 2014 Cost of Cyber Crime Study: United States. 2014.

[2] PwC, Information security breaches survey 2014 - technical report. 2014.

[3] PwC, Managing cyber risks in an interconnected world Key findings from The Global State of Information Security Survey 2015. 2014.

[4] A. Union, The 23rd Ordinary Session of the African Union ends in Malabo - African Union. 2014.

[5] A. Jaquith, Security metrics: replacing fear, uncertainty, and doubt. Upper Saddle River, NJ: Addison-Wesley, 2007.

[6] A. C. S. Associates, Information System Security Attribute Quantification or Ordering (Commonly but improperly known as “Security Metrics”). 2001.

[7] P. E. Black, K. Scarfone, and M. Souppaya, “Cyber security metrics and measures,” Wiley Handb. Sci. Technol. Homel. Secur., 2008.

[8] V. Verendel, “Quantified security is a weak hypothesis: a critical survey of results and assumptions,” in Proceedings of the 2009 workshop on New security paradigms workshop, 2009, pp. 37–50.

[9] S. C. Payne, “A guide to security metrics,” Inst. Inf. Secur. Read. Room, 2006.

[10] D. Hubbard, Measure for measure: The Actuary, official magazine of SIAS and The Actuarial Profession. 2014.

[11] F. Cohen, “Measuring security,” 2011.

[12] T. Kanstrén, R. Savola, A. Evesti, H. Pentikäinen, A. Hecker, M. Ouedraogo, K. Hätönen, P. Halonen, C. Blad, O. López, and others, “Towards an abstraction layer for Security Assurance measurements,” in Proceedings of the Fourth European Conference on Software Architecture: Companion Volume, 2010, pp. 189–196.

[13] K.-E. Sveiby, Methods for Measuring Intangible Assets. 2010.

[14] R. Barabanov, S. Kowalski, and L. Yngström, “Information Security Metrics: State of the Art: State of the art,” 2011.

[15] G. Hinson and K. Brotby, Getting started with security metrics. 2014.

[16] ITU-T, -T X.1520 (01/2014) Common vulnerabilities and exposures. 2014.

[17] R. A. Martin, “Making Security Measurable and Manageable,” Nov. 2008.

[18] T. C. for I. Security, The CIS Security Metrics. 2010.

[19] J. Breier and L. Hudec, “Risk analysis supported by information security metrics,” in Proceedings of the 12th International Conference on Computer Systems and Technologies, 2011, pp. 393–398.

[20] M. M. Gamal, B. Hasan, and A. F. Hegazy, “A Security Analysis Framework Powered by an Expert System,” Int. J. Comput. Sci. Secur. IJCSS, vol. 4, no. 6, p. 505, 2011.

[21] M. Hoehl, Creating a monthly Information Security Scorecard for CIO and CFO. SANS Institute, 2010.

[22] S. Noel and S. Jajodia, “Metrics Suite for Network Attack Graph Analytics,” 2014.

[23] L. Wang, S. Jajodia, A. Singhal, P. Cheng, and S. Noel, “k-Zero day safety: A network security metric for measuring the risk of unknown vulnerabilities,” 2014.

[24] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, Performance Measurement Guide for Information Security NIST Special Publication 800-55 Revision 1. 2008.

[25] P. O. Imeokparia, K. Ediagbonya, and others, “Small and Medium Scale Enterprises (SMEs): A Catalyst in Promoting Economic Development in Nigeria,” J. Educ. Pract., vol. 5, no. 33, pp. 92–98, 2014.

[26] V. Mulango, “SMEs crucial for Africa Transformation Agenda.” Nov-2014.

[27] M. Kimwele, W. Mwangi, and S. Kimani, “Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs),” Int. J. Comput. Sci. Secur. IJCSS, vol. 5, no. 1, p. 39, 2011.

[28] I. S. P. Council, The Basic Policy of Critical Information Infrastructure Protection (3rd Edition). 2014.

[29] DTCC, Cyber risk - a global systemic threat. 2014.

[30] O. of C. and C.- DHS, FY 2014 Chief Information Officer Federal Information Security Management Act Micro Agency Reporting Metrics v1.1. 2014.

[31] O. O. M. A. BUDGET, Annual report to congress: may 1, 2014. 2014.