A Conceptual Framework for the Design of a Nationwide Cyber-Risk Monitoring System

Ebot Ebot Enaw
University of Yaounde I
National Advanced School of Engineering

Djoursoubo Pagou Prosper
University of Yaounde I
National Advanced School of Engineering

ABSTRACT

In recent years, our society has become more dependent on the Internet and ICT in almost every domains (finance, health, education, etc.) making it a major driver of economy growth. However, with the wide adoption of ICT and the Internet, new threats have emerged in the cyberspace called cybercrimes which figure among the key risks factors of companies and governments.

However, due to the complexity of the components of those risks, it is very difficult for top management to get an effective assessment of the risk induced by IT. This in turn jeopardizes the allocation of budget to IT and cybersecurity as well as the prioritization of their related initiatives.

In this light, a system for the automation of risk assessment and monitoring is then highly needed.

In an effort to provide governments and private companies especially those of developing countries with an affordable solution for real time monitoring of the risk level incurred by their information system and to get a nationwide insight of cyber risks, an architecture of a system aimed at automating the collection and centralization of cyber-risk factors nationwide is proposed in this paper.

The novelty of this architecture is that it doesn’t only capture the risks related to individual asset vulnerabilities as other frameworks such as CVSS but in addition proposes an XML schema that captures the risks related to asset vulnerabilities and their attack surface as well as the risks related to attack scenario requiring the combination of breaches of several assets.

This article is structured as follows: section 1 introduces the article, section 2 presents some concepts and works related to the topic covered by the article, section 3 states the problem, section 4 specifies the articles contribution to research, section 5 presents the solution and section 6 presents a case study.

Keywords

Risk, vulnerability, attack surface.

1. INTRODUCTION

Over the past couple of years, the number of cyberattacks and data breaches has considerably increased and so has the damages caused and losses incurred, making cyber risk one of the primary concerns for top management around the world.

Some approaches for risk assessment have been developed but they operated at a strategic level and thus cannot really help in the development of an automated system that will give a clear picture of risks incurred by an information system based on its architecture.

At a more technical or operational level, the Forum of Incident Response Team (FIRST) releases the CVSS standard which defines a set of metrics and a scale to rate the vulnerabilities discovered around the world.

However this standard fails to capture the interconnection between assets as well as the risks related to attack scenario involving the breach of different assets.

In a bid to overcome the aforementioned limitations of CVSS, this paper proposes an architecture of a system aimed at first providing a holistic assessment of the risks faced by an information system by capturing in real time in addition to the CVSS parameters which consider vulnerabilities individually, the parameters related to attack scenario involving the breach of different assets and secondly, centralizing at the national level all the cyber-risk information stemming from public and private companies nationwide.

This architecture can be easily implemented using open sources tools and this will be very helpful for developing countries which lack financial resources to dedicate to cybersecurity.

2. RELATED WORK

Some research has been done on topics related to this issue namely [7] that proposes a review of quantitative and qualitative risk analysis methods. The authors first present the concept of risk analysis with an overview of the different steps entailed namely resources evaluation, identification of vulnerabilities and threats, evaluation of threats probability and consequences. It then defines the concepts of quantitative and qualitative risk assessment before describing some quantitative and qualitative risks analysis methods. The quantitative risk analysis methods presented include: Annual Loss Expected, Courtney and Fischer and ISRAM model. On the other hand, the qualitative methods presented include: FMEA, FMCEA, NIST SP 800-30 and CRAMM. They finally concluded with a comparative analysis that revealed that qualitative methods are easy to implement, quite subjective, cheap but less compatible with a cost/benefit analysis which is very important for managers; whereas quantitative methods are more compatible with a cost/benefit analysis, quite objective but very difficult and expensive to unfold.

[1] After reviewing some risk analysis methods, noticed that the evaluation of risk is compromised by the fact that only the weights of the evaluation criteria which are subjective are taken into account, the weight of objective evaluation criteria were simply ignored. They then proposed a new approach that tackles this issue. The approach consists of the following steps: establish a hierarchical structure model for computer network security risk assessment ; make an evaluation expressed by BPA (Basic Probability Assignment) according to the hierarchical structure model ; determine the subjective weights of criteria and the objective weights of data; obtain comprehensive weights by combining the subjective weights of evaluation criteria and objective weights of data; apply

weighted average combination rule to derive the evaluation result expressed by BPA ; employ PPT (Pignistic Probability Transformation) and principle of maximum membership to get risk level of computer networks. It then illustrated the approach proposed through a case study.

The authors of [8] proposed an approach that combines quantitative risk analysis techniques with qualitative ones. After describing the DDoS attack method they present their qualitative approach that entails assets evaluation, vulnerability assessment, threat assessment, and control assessment. They then describe their quantitative risk analysis approach which is based on the analysis of past data in order to predict present data using conditional probability and Bayesian inference. During the testing phase the observed distribution of data is compared to the expected one using a Q-Q plot that shows the dependency between the observed distribution of data and expected data according to Gamma distribution.

In [6], the authors proposed an architecture for a system aimed at automating the collection of security alerts from a CIRT and vendors and their dissemination to IT managers within security bulletins. The security bulletins designed where customized to the type of assets installed in each information system. Its solution leveraged the CVSS standard for vulnerability scoring, CVE for vulnerability identification and CPE for asset identification. Though its system enables an IT administrator to get a clear picture of the vulnerabilities inherent in its information system and their scoring, it did not capture the risks posed by the interconnection between different assets.

In [3], while pointing out the variation between different studies in the estimated direct and systemic costs of cyber incidents, which is complicated by the considerable variation in cyber risk across countries and industry sectors the authors proposed a transparent and adaptable methodology for estimating present and future global costs of cyber risk that takes into account the considerable uncertainty in the frequencies and costs of cyber incidents. Their methodology consists of first identifying the value at risk by country and industry sector; then computing direct costs by considering multiple financial exposures for each industry sector and the fraction of each exposure that is potentially at risk to cyber incidents; and finally computing the systemic costs of cyber risk between industry sectors using Organization for Economic Cooperation and Development input, output, and value-added data across sectors in more than 60 countries.

In an effort to tackle the issues of lack of historical data that hampered the development of a sustainable cyber-insurance, the authors of [4] proposed a tool named CRISM that produces risk scores that can be used by insurance underwriters and also by enterprise risk managers and information security officers to prioritize cyber risk mitigation. This tool first maps system and network using nmap, then identifies all the vulnerabilities inherent in the systems and assets discovered and further produces the Bayesian attack graph using Bayesian belief network and finally computes the overall enterprise cyber risk score.

In [2] the authors hypothesize that most of the vulnerabilities inherent in software at any time are undiscovered and that most risk assessment methodologies are based only on known vulnerabilities which then compromise their efficiency. In an effort to prove their hypothesis, they propose a metric aimed at estimating the total number of unknown or latent vulnerabilities in large software. The metrics used are based on several parameters such as the number of line codes, the flaw rates and the number of known vulnerabilities.

Therefore, in order to tackle these issues, this paper proposes an architecture of a system aimed at computing in real time the holistic risk assessment of an information system by capturing in addition to common CVSS metrics, other metrics related to the interconnection of assets and attack scenarios involving the breach of several assets.

2.1 Risk Assessment

Risk can be defined as the combination of the likelihood of an attack causing damage and the level of the damage should it occur.

There are two main categories of risk evaluation methods namely quantitative risk analysis methods which are mathematical approaches that assign monetary and numeric values to risks and qualitative risk analysis methods which are more opinion- and scenario-based and use a literal rating system to capture the risk level.

Table 1: qualitative risk analysis matrix

Likelihood	**Consequences**				
	Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
Almost certain	**M**	**H**	**H**	**E**	**E**
Likely	**M**	**M**	**H**	**H**	**E**
Possible	**L**	**M**	**M**	**H**	**E**
Unlikely	**L**	**M**	**M**	**M**	**H**
Rare	**L**	**L**	**M**	**M**	**H**

There are so many methods of risk evaluation namely CRAMM, OCTAVE, FRA, etc. but they all do not address one of the aforementioned category.

To evaluate risk, one has to identify vulnerabilities and threats and the value of the assets, then evaluate the probability of the exploitation of vulnerabilities by threats as well as the losses and damages caused by the successful exploitation of these vulnerabilities. The detailed process of risk evaluation is depicted in figure 1.

It is worth mentioning that in addition to providing a measure of the impact of cyber threats to the business, Risk evaluation also provides to top management with a tool to prioritize the risks with regards to budget constraints as well as enable them to have a clear visibility of the budget allocation to cybersecurity through a cost/benefit analysis assessment process .

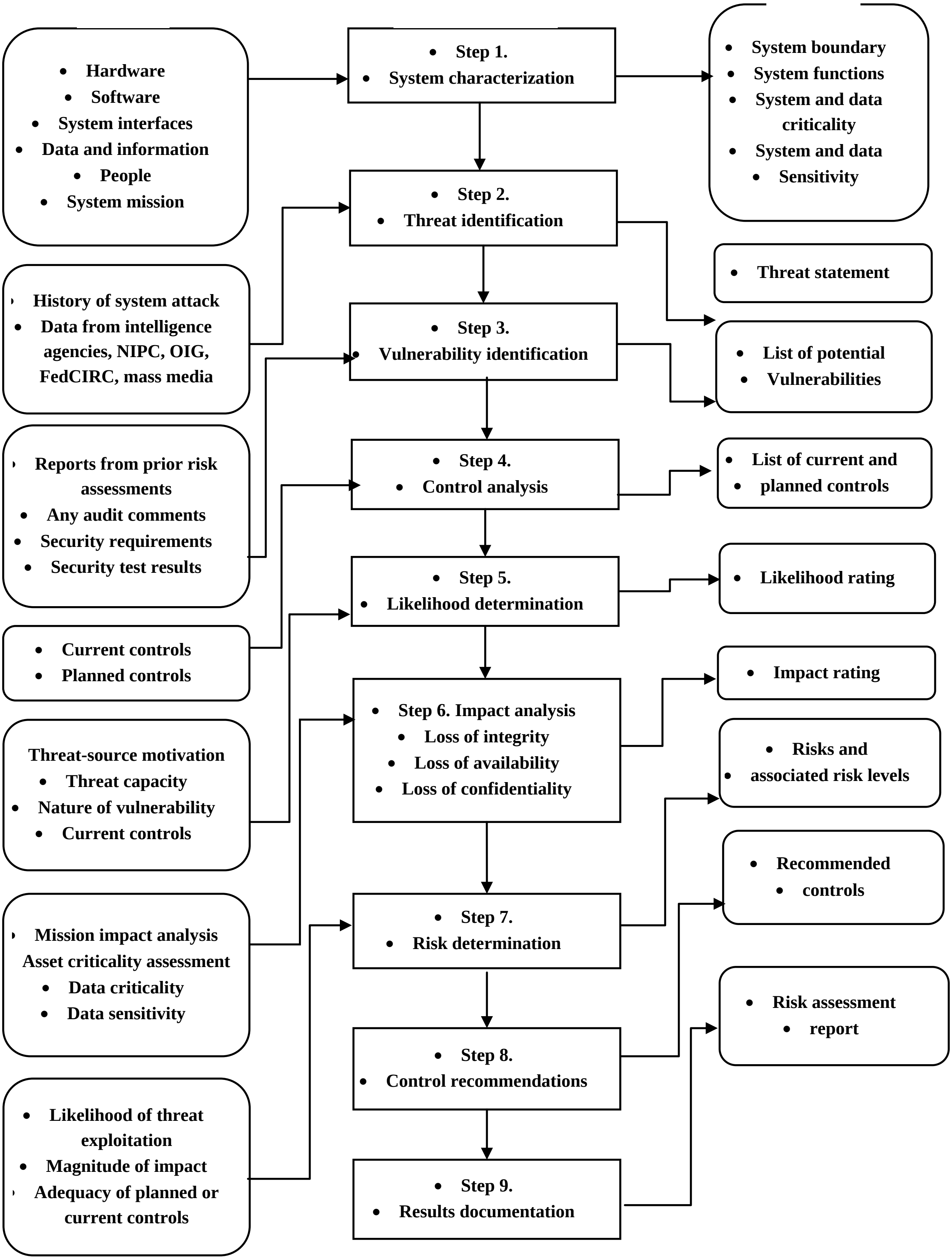

Figure 1: Risk assessment workflow

2.2 Risk Management

Information risk management (IRM) can be defined as the perpetual process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.

Thus as recommended by the ISO 27001 standard, prior to conducting risk management, acceptable level of risk needs to be identified. The identification of acceptable level should be based on the business process because the IT is an enabler for business so it should be aligned to business and the risks posed by IT should be analyzed from the perspective of business. The acceptable level of risk will then serve as a control value of risk management since the target is to have a risk that is lower or equal to the acceptable level.

Globally, risk management is one of the most important activity in the daily operations of a manager. Due to the omnipresence of ICT in almost every domain, IT risk has become one of the most important component of business risk. Depending on the result of the risk evaluation phase, top management can choose either one of the following actions:

- Accept: the risk can be accepted if the risk level is less than or equal to the acceptable level of risk of that company or if the cost to patch the vulnerability is greater than the loss incurred by that risk ;
- Remediate: This action consists of applying specific corrective measures so as to mitigate the risk or bring it to the acceptable level ;
- Eliminate: This action consists of eliminating the assets that are targeted by a specific risk ;
- Transfer: This action consists of subscribing to an insurance policy that will handle the damage if the threats successfully exploit the vulnerability.

2.3 CVSS

According to CVSS [7], the assessment of risks posed by a vulnerability to an asset requires a set of metrics or indicator that can be categorized into three (03) major groups called vectors:

- Base vector: It represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the Exploitability metrics which reflects the ease by which the vulnerability can be exploited and the Impact metrics which reflects the direct consequence of a successful exploit. Among the Base vector metrics, we have: the attack vector, the attack complexity, the privilege required to launch the attack, the level of user interaction required, the scope, the impact on confidentiality, integrity and availability ;
- Temporal vector: It reflects the characteristics of a vulnerability that may change over time but not across user environments. Among the temporal vector metrics we have: the exploit code maturity, the remediation level and the level of the confidence in the report that disclose the vulnerability ;
- Environmental vector: It represents the characteristics of a vulnerability that are specific to a particular user's environment. Among the environmental vector metrics, we have the requirement in confidentiality, integrity and availability, the modified attack vector, the modified attack complexity, the modified privilege required to launch the attack, the modified level of user interaction required, the modified scope, the modified impact on confidentiality, integrity and availability.

3. RESEARCH PROBLEM

Given the surge in cybercrimes and the ever-growing importance of Information System for business processes, companies and governments are more than ever in need of a system that can provide a concise evaluation of their cyber risk at any time.

Generally, to assess their cyber risk, companies and governments gather security alerts related to the latest vulnerability discovered that are related to their assets or carried out vulnerability scanning which enable them to identify the vulnerabilities inherent in their assets.

One of the most prominent standard for vulnerability’s risk rating is CVSS which has been designed by the Forum of Incident Response Team to help CIRT, and solutions provider to compute the severity of the risk induced by a vulnerability based on a set of metrics classified in three (03) main vector: base vector, temporal vector and environmental vector.

However CVSS rates vulnerabilities individually, it does not take into account the interconnection of the assets and risks related to attack scenario requiring the breach of several assets and so does not provide a clear picture of the whole risk an information system is subjected to. Moreover, it is very vulnerability-centric and does not consider the attack surface of the assets which play an important role in the assessment of risks.

4. CONTRIBUTION TO RESEARCH

The paper’s contribution is twofold:

Firstly a framework for the holistic assessment of technical risk associated with an information system is proposed. The said framework not only takes into account the risks factor of individual vulnerabilities inherent in individual assets as CVSS does but also the factors that express the risks related to the interconnected nature of an information system and the attack scenario requiring the breach of different assets.

Secondly, an architecture of a system that on the one hand enables public and private companies to build their risk assessment and follow-up platforms and on the other hand enables interoperability and exchange of risks factor’s information among these platforms via the XML protocol.

5. THE SOLUTION

5.1 Overview of the Framework

In an effort to provide IT managers with a system that allows them to manage and follow on a daily basis data related to their IT assets risks in a holistic manner as well as allow national CIRT have a clear picture of the risk level associated with critical infrastructures at the national level, an architecture of a system that leverages a framework that captures the main components of IT risks is defined in this paper.

It is worth mentioning that though IT risk depends on several types of threat agents namely technical, natural, human and organizational, in this paper only the technical threat agents are considered. So the scope of the framework is limited to risks induced by technical vulnerabilities and threats.

The workflow of the system proposed can be described as follows:

1. Collect the information about the different assets of an information system
2. Gather in real time the vulnerabilities that target each of the asset with their CVSS metrics

3. Identify the metrics not included in CVSS and that capture the attack surface of each asset as well as the logical and physical interconnection between assets and the risk induced by attack scenario involving the breach of several assets
4. Transmit the data to the Central Risk Assessment System of the National CIRT through a protocol based on XML

From this workflow, a system made up of four (04) main modules namely: vulnerability descriptor, assets descriptor, synthetizer and Central Risk dashboard is presented. The architecture of the system is depicted below.

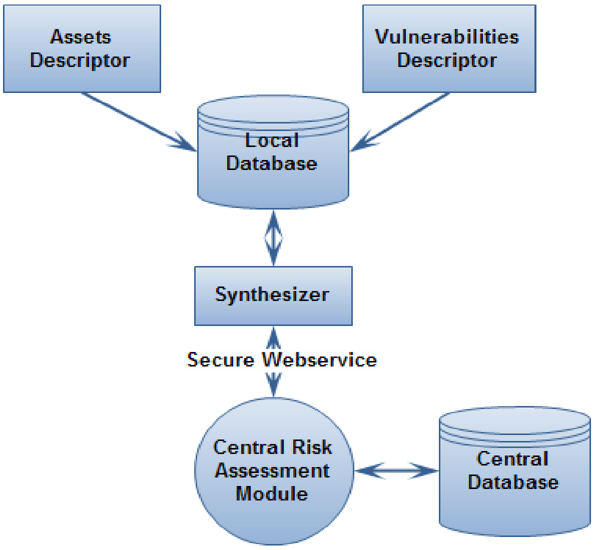

Figure 2: Architecture of the system at a local level

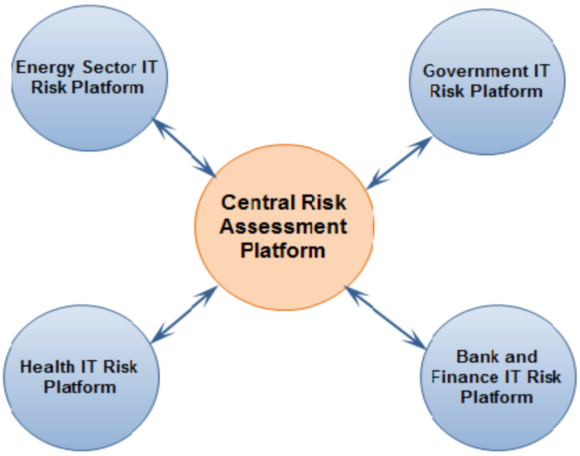
Energy Sector IT Risk Platform
Government IT Risk Platform
Central Risk Assessment Platform
Health IT Risk Platform
Bank and Finance IT Risk Platform

Figure 3: Architecture of the system at the national level

5.2 Vulnerability Descriptor

This module is in charge of the collection of the vulnerabilities related to the different assets of the information system and their storage in a local database. It is structured in an abstract way so as to be able to collect vulnerabilities disclosed in several sources.

For the vulnerabilities scoring, this module relies on the CVSS standard.

Unlike CVSS which associates the environmental metrics with vulnerabilities, the proposed framework however associates the environmental metrics with assets since these metrics are specific to the architecture of an information system which captures the environment.

Given that the temporal metrics change over time, this module is in charge of updating these metrics whenever there are new information namely the release of new patches addressing a given vulnerability.

It is worth mentioning that CVSS only deals with individual vulnerability and so does not capture risks related to attack scenario involving several vulnerabilities targeting different assets. Since the paper’s objective is to design a framework that handles risks in a holistic manner, CVSS is complemented with other parameters that address these issues. These aspects are taken into consideration in the asset descriptor module.

5.3 Asset Descriptor

This module is aimed at capturing the architecture of the entire information system and its specificity in a bid to capture the elements that will allow for an objective assessment of the risk level incurred by an information system in a holistic manner.

Two assets of the same type with the same vulnerabilities might not induce the same risk level depending on the environment or the architecture of the information system where they are found. This module is intended to capture the specificity of a particular environment, the interconnections between assets in the evaluation of the risk incurred by the whole information system. It thus complements CVSS which treats assets and vulnerabilities individually.

Thus, this module takes into consideration the metrics of the CVSS environmental vector and other metrics that express the risks induced by the interconnections between assets and attack scenario involving the breach of several assets.

Therefore the factors taken into account are:

- the technical specification of the assets,
- the value of the asset to the organization and its requirement in terms of confidentiality, integrity and availability: the estimation of the value of an asset should take into consideration several parameters namely the cost to acquire or develop the asset, the cost to maintain and protect the asset, the value of the asset to owners and users, the value of the asset to adversaries, the price others are willing to pay for the asset, the cost to replace the asset if lost, the shortfall induced by a compromise on confidentiality, integrity or availability of the asset ;
- the attack surface of assets: It can be defined as the total number of points or vectors through which an attacker could try to enter an environment. It plays an important role in the assessment of the whole risk incurred by an information system ;
- the physical and logical interconnection of the assets with others. Some attack involve the exploitation of several vulnerability inherent in different assets, so in order to get a good estimation of the level of risk induced by these types of attack, it is indispensable to take into consideration the physical and logical interconnection of assets.

Assets are classified into five (05) main categories namely:

- Data
- Software
- Operating systems
- Processing equipment which encompasses equipment like PC and servers

- Networking equipment which encompasses like switch, firewall, etc.

After collecting the information related to the assets and the information system’s architecture, the module stores them in a local database.

In our system, the description of each of these entities will include the link to the other entities on which the entity in question depends. For example, since data is processed by a software which is run on an operating system that is installed on a computer or a server, the description of the software will include links to the data that it handles, the description of an operating system will include links to the software that are installed on it and the description of the computer or server will in turn include links to the description of the operating systems that are installed on it.

5.3.1 Data

Data is the main asset on which other assets depend because every information system is generally aimed at taking data as input, process it and output the result. The risk incurred by other assets depends heavily on the type of data that passes through it and their security requirements.

Thus the proposed framework uses the following parameters to specify data:

- The value
- The requirement in terms of confidentiality
- The requirement in terms of integrity
- The requirement in terms of availability

Other parameters like the id that identify the data, the description of the data and the identifier of the software that processed it are also taken into consideration.

5.3.2 Software

Software is one of the most important assets in an information system, since it processes data and delivers the services required by businesses. When assessing the risks incurred by a software, several parameters are considered namely:

The CVSS environmental parameters which include:

- The requirements of software in terms of confidentiality, integrity and availability of the process it implements ;
- The measures deployed to mitigate the effect of some vulnerabilities

Additional parameters associated with the proposed system include:

- The attack surface of the software in question.
- The id which is the parameter that identifies uniquely a particular software in an information system, the name of the software, the version, the id of the patches applied, the CPE-ID, the id of the data taken in input and submit as output

  To define the attack surface, we use several parameters:

- the fields of the different forms of the software as well as the type of data processed by a given form,
- the logical interfaces of the software which are defined as the set of IP+Port Number+Protocol from which the software receives data or to which it transmits. This specific parameters capture the set of softwares, databases or other platforms with which the software in question interacts
- The technologies, framework and API used to develop the software in question
- The operating system and virtual machine on which the software is installed

5.3.3 Operating System

Operating systems manage all the logical assets of a computer as well as their interactions and the physical and logical resources. Thus, they play an important role in an information system and as such account for most of the risk associated with businesses. The proposed framework uses the following parameters to model Operating System:

The CVSS parameters including:

- The requirements of the OS in question in terms of the confidentiality, integrity and availability ;
- The measures deployed to mitigate the effect of some vulnerabilities.

Additional parameters unique to the proposed system include: the name of the OS, its version, the id of the patches applied, the file system and the attack surface.

The attack surface of an OS is essentially made up of:

- o the logical interfaces of the OS which are defined as the set of IP+Port Number+ Protocol from which the OS receives data or to which it transmits.
- o The technologies, framework and API used to develop the operating system in question
- o The virtual machine on which the operating system is installed
- o The physical device on which the operating system operates

5.3.4 Processing Equipment

This category of equipment encompasses devices like server, personal computer, smartphone and tablets. The parameters used to model processing equipment include:

The CVSS parameters including:

- The requirements of the equipment in question in terms of confidentiality, integrity and availability ;
- The measures deployed to mitigate the effect of some vulnerabilities.

Additional parameters include: the brand of the terminal, the processor used, its identifier and the attack surface which is made up of the following items:

- o The firmware of the device as well as the BIOS OR UEFI ;
- o The physical interface of the device whether USB, Ethernet, wireless, VGA, etc, their status and physical access control implemented on them. It is worth mentioning that every logical interface is associated with a physical interface

5.3.5 Networking Equipment

The networking equipment enable the other assets of the information system to communicate and as such have an important impact on the overall risk. The parameters used to model the risk induced by a networking equipment include:

The CVSS parameters which are:

- The requirements of the equipment in question in terms of the confidentiality, integrity and availability ;
- The measures deployed to mitigate the effect of some vulnerabilities.

Other parameters include:

- The forwarding rules: it expresses the type of session flow (source to destination) that are allowed in the equipment. The source and destination can be defined in terms of IP+port or in terms of physical interface
- The access control rules: it expresses the type of session flow (source to destination) that are denied. The source and destination can be defined in terms of IP+port or in terms of physical interface.
- The attack surfaces which is mainly defined by the following items:
    - The physical interfaces of the device, their status and physical access control implemented on them.
    - The physical and logical interfaces through which the equipment can be managed or the configurations can be set
    - The operating system and firmware that run on the equipment

Other parameters such as the id which uniquely identifies the equipment, the OSI layer at which the device operates, the name and the brand, the version and patches installed are also taken into consideration.

5.3.6 *Security Solutions*

It encompasses all the cybersecurity solutions deployed in the information system whether material or software. The parameters used to model the risk factor of Security solutions in the proposed framework include:

The CVSS parameters which include:

- The requirements of the security solutions in terms of confidentiality, integrity and availability ;
- The measures deployed to mitigate the effect of some vulnerabilities.

Additional parameters include:

- The type of the equipment
- The physical interfaces of the device, their status and physical access control implemented on them
- The physical and logical interface through which the equipment can be managed or the configurations can be set
- The operating system and firmwares that run on the equipment
- The fail close or fail open status
- The access control rules which expresses the type of session flow (source to destination) that are denied or inspected. The source and destination can be defined in terms of IP+port or in terms of physical interface while the inspection is defined in terms of signature or behavior recognized. The action carried out by the equipment in case of a signature match (block, log, alert) is also taken into account.

Other parameters such as the id which uniquely identifies the equipment, the OSI layer at which the device operates, the features deployed (antivirus, IPS, IDS, Honeypot), the name and the brand, the version and patches installed are also taken into consideration.

5.4 Synthetizer

This module is in charge of gathering information related to assets and vulnerabilities, collected by the previous modules and then structuring them in XML schemas, which are transmitted to the Central Risk Assessment System of the National CIRT using secured web services. This module is also in charge of evaluating the impact of the risk associated with an asset on the confidentiality, integrity and availability.

Concerning the impact on availability, since the availability of an asset depends on the availability of all the assets that sit on the path to that particular asset, to determine the impact on the availability of an asset, this module will combine the availability impact of all the vulnerabilities inherent in the other assets that sit on the path of the asset in question. The availability impact value used will be that of the environmental vector of CVSS which is captured in the asset descriptor module.

With regard to confidentiality and integrity, since in order to compromise the confidentiality or the integrity of an asset, the attacker should first of all gain access to the asset, it is therefore necessary to combine the physical and logical accessibility to the asset with the confidentiality and integrity impact of the asset. The accessibility to the asset is evaluated through the combination of the physical and logical path to the asset as well as the permissibility of the asset that sits on its path. For example, to gain access to an internal server of a company, the hacker will need to compromise the networking and security equipments that sit between him and the server so as to modify their configurations which might necessitate appropriate exploits code that use specific vulnerabilities inherent in these equipments and that can allow the attacker to modify the configuration of these equipments. So in this case, the module will take into account the physical and logical paths to the internal server in question as well as the environmental vector metric of all the vulnerabilities that were exploited to modify the configurations of the networking and security equipment.

5.5 Central Risk Assessment

This module is in charge of gathering the information related to the different assets and their vulnerabilities from public and private companies of the country. It is aimed at providing a global picture of the risks associated with the IT assets and critical infrastructure nationwide.

It will be particularly useful in the prevention of risks related to coordinated attacks against critical infrastructures of a country.

It is worth mentioning that this module is also in charge of handling the risk associated with the interconnection of assets belonging to different companies.

6. CASE STUDY

Through the Synthetizer module the system proposed above permits to assess the risk induced by a vulnerability on an entire information system by taking into consideration the interconnections between assets.

For example, if the system is run with the data related to the information system below (*figure 4*).

1. The asset descriptor module will provide the following information (name, OS, ports, etc) of all the assets which include: The two switches, two servers and two

workstations. This module also provides information related to the logical and physical links between these assets ;

2. The vulnerability descriptor module provides information related to all vulnerabilities that target each of the assets with their CVSS base and temporal metrics. Thus, the native impact of these vulnerabilities on the availability, confidentiality and integrity is evaluated and stored in the local database of the organization hosting the information system in question. For illustration purposes, it is assumed that two switches have two main vulnerabilities CVE 2010-3050 and CVE 2017-12240 that can respectively lead to a denial of service and a remote code execution ;
3. The synthetizer module retrieves and analyzes data previously stored in the local database by the Asset and Vulnerability descriptor modules. It then establishes the associations between assets and the vulnerabilities that target specific assets and the topology of the information system. It could for example reveal that the exploitation of the CVE 2010-3050 vulnerability in SWITCH A could lead to the unavailability of all the servers located in the server farm since the only way to get to these servers is through SWITCH A. Also, it could reveal that the exploitation of the CVE 2017-12240 vulnerability on SWITCH B could allow an attacker to modify the configuration of the SWITCH and overwrite access-list which can grant an unauthorized PC access to one of the servers. This evaluation would never have been possible with CVSS since it can only address vulnerabilities associated with a unique asset as opposed to our system which addresses vulnerabilities in a holistic manner.

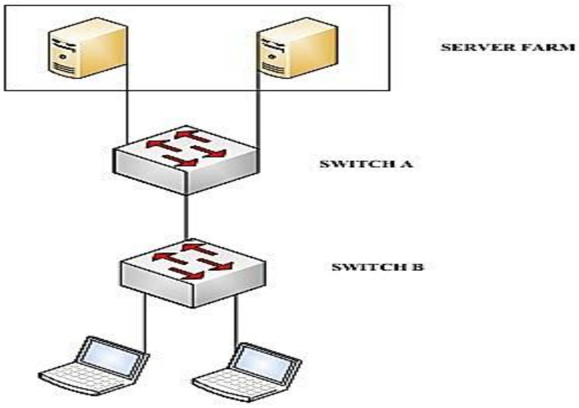

Figure 4: Case study archtiecture

7. CONCLUSION AND FUTURE WORK

The widespread use of ICT and the Internet and the rapid development of E-business, combined with the surge of cybercrimes worldwide has made IT risk one of the key component in business risk assessment.

Continually assessing and monitoring the global level of risk of an information system is therefore a challenge especially given the diversity of assets involved and their logical and physical interconnections.

To this effect, in this paper an architecture of a system to automate the assessment and follow-up of the risk associated with an information system in a holistic manner is proposed.

The said architecture leverages a framework that provides a model in XML of the metrics that can be used to grasp the holistic IT risk level. In this light, it is based on two main entities namely the vulnerabilities whose metrics are inspired from the CVSS standard and the assets whose properties express the specificities of the information system architecture and the interconnected nature of an information system so as to take into consideration the risks related to various attack scenario involving the breach of several assets.

For every asset, the framework tries to capture among others, the requirements in terms of confidentiality, integrity and availability, its attack surface and the logical and physical interconnection with other assets. As opposed to CVSS, the proposed framework doesn’t only take into consideration risk induced by vulnerabilities in an isolated manner but it tries to capture the holistic information system risk and therefore takes into account the attack surface of assets and the physical and logical connection between assets.

Future work could include the application of model checking techniques to our framework in a bid to provide a formal model of undesired properties and thus identify the attacks scenarios with their corresponding risk evaluation.

8. REFERENCES

[1] Yancui Duan, Yonghua Cai, Zhikang Wang, Xinyang Deng. 2018. A novel network security risk assessment approach by combining subjective and objectivve weights under uncertainty in MDPI applied sciences

[2] Thomas Llanso, Martha McNeil. 2018. Estimating Software Vulnerability Counts in the Context of Cyber Risk Assessments in Proceedings of the 51st Hawaii International Conference on System Sciences

[3] P.Dreyer, T.Jones, K.Klima, J.Oberholtzer, Aaron Strong, J.W Welburn, Z.Winkelman. 2018. Estimating the Global Cost of Cyber Risk Methodology and examples in RAND

[4] Sachin Shettya , Michael McShanea , Linfeng Zhangb , Jay P. Kesanb , Charles A. Kamhouac , Kevin Kwiatc and Laurent L. Njilla, 2018. Reducing Informational Disadvantages to Improve Cyber Risk Management in Geneva Papers

[5] Gante Wangen, Andri Shalaginov, Christoffer Hallstensen, Xinyang Deng. 2016. Cyber security risk assessment of a DDoS attack in International Conference on Information Security.

[6] Ebot Ebot Enaw. 2014. A system for collecting security alerts and diffusing customized security bulletins in International Journal of Advanced Computer Technology, volume 3 Issue 2.

[7] Artur Rot, 2008. IT Risk assessment: quantitative and qualitative approach in Proceeding of the world congress on Engineering and Computer science.

[8] Forum of Incident Response Team, “Common Vulnerability Scoring System (CVSS) v3.0" https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf.