I. Introduction

There is a growing concern with information security, resulting in the growth of a new field – technology risk analysis. The role of a technological risk analyst is to identify vulnerabilities, calculate a vulnerability score and verify whether or not the identified vulnerability could affect a business. If so, he or she must correct the problem expeditiously. Though this task may appear simple at first glance, with relatively few steps to follow, the number of vulnerabilities has been increasing exponentially to the point that it has become impossible to identify vulnerabilities in a manual or even semi-automatic manner. It is also important to note that there is an increasing demand for risk analysis transparency by the market and by regulatory bodies that require corporations to follow strict information security management norms, such as Sarbanes–Oxley (SOX)[4], Basel Accords I and II[10], ISO 17799[1], ISO 27001[7] and BS–7799[2]. The need to adhere to international norms may result in extra costs and, in some cases, loss of competitiveness, albeit typically only in the short term. Medium and long-term effects resulting from the implementation of such norms are clearly beneficial and demonstrate a certain business “maturity” and preparedness that may even attract new investments and increase the trust of stakeholders.

Abstract - The growing need for transparency in business negotiations requires greater control of technological risks. However, technological risk assessment tools currently available in the market are imprecise as they are based on the analysis of events that have already passed. The current paper describes a real-time, proactive risk analysis framework. We propose that instead of testing vulnerabilities from an external point of view, agents be incorporated and distributed into “actives” (hardware and software) so as to be able to provide application, configuration and specific localization information. In this manner, changes noted will be divulged by the agent in an immediate and pro-active manner to a central repository. When vulnerabilities are detected, correction processes will be implemented automatically, permitting technological risks to be monitored in real-time.

Key words: Risk assessment, information security, real time, vulnerability analyst.
The growing need for transparency in business requires greater control of technological risks. Risk can be defined as the probability that a physical situation will cause damage, at any level, during a specified period of time of a vulnerability, which, in turn, is defined as a weakness in the system that may involve people, processes or technology that can be exploited to obtain access to information. The existence of a vulnerability creates a risk that results in a threat, here defined as any circumstance or event that has the potential to cause an impact on the confidentiality, integrity or availability of information. As such, the proper classification of information is of critical importance in the cycle of security processes.

Risk analysis may be extremely complex and is directly dependent on proper planning and prior knowledge of the technological environment in which the analysis will be undertaken. And as such, it is defined as a process that aims to identify, analyze, reduce or transfer risk [13]. The technological risk analysis tools currently available in the market are highly dependent on proprietary operational systems [15][16] that tie the “solution” to a single platform. Additionally, these tools base their assessment on collected information regarding past events and, consequently, are unable to provide a true solution in real time.

Contrary to static models of risk analysis, this paper proposes a pro-active framework that functions in real-time. Instead of testing vulnerabilities from an external point of view, where the information is obtained by simply exploring the “active” (computational system composed of hardware and software), we propose that agents (sensors) capable of providing application, configuration and localization information be incorporated into actives. Any observed changes, such as physical location, software update or installation, hardware modifications, changes in security policy, etc., will be immediately reported by the agent, in a pro-active manner, to a central repository. The function of the central repository will be to correlate the information provided by the agents with vulnerability information published by the National Institute of Standards and Technology (NIST) through a Common Vulnerability Scoring System (CVSS). Should a vulnerability be identified, a correction process will be immediately requested and the team responsible for that particular active will initiate laboratory analysis in order to make appropriate corrections.

The current paper is structured in the following manner: In Section 2, we present published work that is relevant to the topic. Section 3 will further explore the use of CVSS as an initial methodological base, as well as the metrics used for risk analysis. The model used to register vulnerabilities, known as Common Vulnerabilities and Exposures (CVE) will be discussed in Section 4. Sections 5 and 6 will address means to obtain and classify inventories as well as further detail the methodology of the proposed framework. Finally, Section 7 will present the conclusion and the direction of future work.

II. Related works

During the development of this work we did not identify any previous works that proposed to conduct a risk analysis of information assets in real time, that is, at the very moment that a vulnerability is identified and reported. In this context, we describe below the publications that contributed to meeting our original objective. The information necessary to define risk and security was established in a recent study by Perera and Holsomback [9]. The study further suggested a matrix for risk analysis following the framework shown in Figure 1.

The authors also proposed a risk management system based on IRMA1. However, this system is limited in that risk input must always be done manually; consequently there is always the need for a risk analyst to input information.

A study by Fussell and Field [6] identified and described methods for risk analysis management. However, similar to that noted by Perera and Holsomback [9], the described method was

---

1 Intergovernmental Risk Management Agency
limited in that there was no systematic automation for system data collection to be used in risk management. The OCTAVE method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) was described previously [14]. Briefly a team, known as an “analysis team”, managed the process and analyzed the information, taking direct action when called for, depending on the situation. The method consisted of three distinct phases:

1. The characterization of a threat profile, during which the network structure and information organization are identified and described.
2. Identification of vulnerabilities, during which the infrastructure is evaluated and vulnerable points are identified.
3. Strategy planning and development of a security plan, during which the critical work of developing a risk analysis plan of action is completed.

The difficulty in implementing this method is related to the need for a team of people to work exclusively in the analysis of information and risk so that decisions can be made. The objective of this paper is to provide a detailed discussion of a methodology that permits risk analysis calculations for applications and equipment in the area of information technology through the use of sensors that will collect local information and store the data in a central repository. Comparisons between the information provided by the sensors with available vulnerability information in databases will permit the identification of vulnerabilities in real-time, facilitating the initiation of correction processes.

III. Common Vulnerability Scoring System

Various information security departments such as the NIST (National Institute of Standards and Technology), FIRST (Forum of Incident Response and Security Teams) and CERT (Computer Emergency Response Team), etc., have created a standard with which to measure and quantify software vulnerabilities, known as CVSS [11]. Historically, the industry has utilized various scoring methods to determine software vulnerability [8]. However, the criteria or processes used were not detailed, which has caused serious problems to users in the management of their systems and applications. It is important to note that all variabilities exist within a limited timeframe, which must be acknowledged in order to solve problems. The current work utilized CVSS and was based on the assumption that there will be standardization of vulnerability information and reporting of errors. Information divulged by CVSS will be stored internally and immediately compared with inventoried information, identifying actives that may be vulnerable.

FIRST was chosen by the NIAC (National
A framework for risk assessment of information technology in the corporate environment

Infrastructure Advisory Council) to head the CVSS project and to establish an open and universal evaluation standard to help organizations prioritize security and vulnerability analysis issues. The goal was to consolidate the efforts of security teams world-wide to solve the standardization problem and to facilitate a quicker response time in addressing risks to known vulnerabilities. CVSS utilizes the following three basic metrics to calculate the score of a given vulnerability:

- Base metrics: contain the attributes that are intrinsic to all vulnerabilities.
- Temporal metrics: contain the vulnerabilities that evolve over time and are dependent upon the lifecycle of the vulnerability.
- Environmental metrics: represent those characteristics that are unique to the corporate environment in which they are being considered.

A. Base metrics

Base metrics are established by the manufacturer; they are based on the functionality and use of each software, and can be adapted to meet certain criteria. A total of seven impacts (summarized below) are used to obtain a final score that, in conjunction with the temporal and environmental metrics, will comprise the final risk score.

1. Access difficulty: measures the complexity required for a hacker to explore the targeted system.
2. Access vector: determines whether or not the vulnerability can be explored locally or remotely.
3. Authentication: determines whether or not an intruder needs to obtain authentication to explore the vulnerability of the system.
5. Integrity impact: determines the impact on data integrity.
6. Availability: determines the availability impact.
7. CIA impact (Confidentiality, Integrity, Availability): permits the evaluator to give greater weight to one of the CIA scores relative to the others.

B. Temporal metrics

Events may occur that affect the urgency of the threat posed by the vulnerability during the lifecycle of a vulnerability.

1. Exploitability. This assessment determines whether or not it is possible to exploit the vulnerability. Exploitability can be classified as one of the following:
   a. Unproven: without a known exploit.
   b. Proof of concept: a concept text has been created, suggesting that a threat exists.
   c. Functional: when a known exploit is in existence.
   d. High: when the vulnerability is actively being exploited manually or by a malicious code.

2. Remediation level. This assessment provides information as to whether or not a solution has been identified.
   a. Official fix: manufacturer-provided correction (patch)
   b. Temporary fix: manufacturer-provided temporary solution
   c. Walkaround and unavailable

3. Report confidence. This assessment represents the degree of credibility that a vulnerability exists and the credibility of its dissemination (Unconfirmed/Uncorroborated/Confirmed)

C. Environmental metrics

Environmental metrics are the only metrics that are defined based on the situation of the specific company and consequently can be manipulated and changed by managers, auditors and consultants to more accurately represent the reality of a given company.

1. Collateral Damage Potential. This assessment measures potential damage, which can represent the risk of loss of equipment and property damage.
2. **Target Distribution.** This assessment indicates the percentage of systems, relative to the number of systems, that are susceptible to the vulnerability (None; Low, up to 15%; Medium, up to 40%; High, over 50% of the systems are vulnerable).

**D. Scoring process**

The scoring process will define a final value based on a combination of all the metrics used, combining the values utilizing pre-determined formulas [11]. The final score is obtained by combining the three previously described CVSS groups. The metric system can be defined by the vectors listed in Table 1, facilitating the input of data and its use by a managing program.

**IV. Common Vulnerabilities and Exposures (CVE)**

The CVE is a public database in which anyone can obtain information on vulnerabilities. It has defined standards relative to the treatment and dissemination of vulnerability information. The CVE database is the result of collaborative efforts between various entities working with information security, such as the Sans Institute, Cancert, and CERT, among others. Massachusetts Institute of Technology’s Digital Computer Laboratory (MITRE) is the main custodian of CVE. Given that this is a collaborative project, no pre-specified contributions are expected. However, financial contributions as well as assistance in disseminating information are permitted.

MITRE’s main objective for CVE is not simply for it to disseminate information regarding vulnerability and security, but for it to standardize the manner in which this information should be treated. CVE should prevent duplication of information and enable optimal utilization of the collected data. Thus CVE is capable of providing a more comprehensive database and consequently better quality data security.

**V. Management of resources**

According to the ISO 27001 normative of 2005, all of a company’s informational resources must be identified and managed based on previously established determined controls. Ideally, informational resources should be documented and categorized according to their level of importance. The consequences of a particular resource being compromised must also be considered. An effective risk analysis starts from the premise that the full technological infrastructure has been identified [3]. There are various manners in which this can be accomplished, such as through manual research of the network, through speaking and interviewing those directly responsible for the infrastructure, through contacting the connections points, and through identifying and recording all of the components of the network.

Risk management is a neverending process that must continuously be reevaluated to identify any inconsistencies. The process of risk analysis itself can be divided into six parts (Figure 2).

It is reasonable to assume that it would be viable to implement the above-mentioned points with a small to medium size network (up to 1000 machines). Unfortunately, as soon as the data collection process has been finished and the risk scoring initiated, the analysis would already be outdated—that is, that which was assessed would already be in the past. Every passing minute makes

<table>
<thead>
<tr>
<th>Table 1. CVSS vector definition [11].</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vector</strong></td>
</tr>
</tbody>
</table>
risk analysis less efficient. As such, risk analysis may provide a false sense of security. The proposed framework addresses this issue by allowing a real time analysis of the known vulnerabilities and the latest inventory changes.

5.1 Inventory procedures

The speed, at which information can be collected and updated, as a result of constant changes, is the key to successful risk analysis. Ideally, inventory tools used should meet the following requirements:

- Possess a characteristic client/server support system
- Be a central database where all the information is stored
- Be a multiple platform, accessible to diverse systems
- Be manageable in such a way that information can be requested and obtained at any time.
- Consume a minimum amount of resources to maintain proper functioning of the client’s system
- Have the capacity to inform, even if the client is disabled
- Have the ability to be reconfigured at any moment, in a global manner and independent of the user

Apart from these initial requirements, the tool must also have the capacity to collect diverse information for the inventory; all collected information should be sent to the central database. Essential information includes:

- Version of the operating system
- Any corrections made and the respective version of each
- Information about registered and former users
- List of all installed software and software versions
- Verification of installed antivirus systems and updates
- Partition information
- User-provided descriptions of the physical locations of hardware components
- Descriptive list of hardware components, including memory capacity, processor speed, hard drive capacity, and video card specifications

Following data collection to obtain the basic characteristics of the IT infrastructure, qualification of each component must then be done, based on the following categories of importance:

1. Irrelevant
2. Relevant
3. Important
4. Critical
5. Vital

VI. Proposal Framework

The objective of this article is to report a methodology for the collection, treatment and presentation of data regarding vulnerabilities, correlating events with information obtained from an internal network. To this end, two diagrams have been created, one from the point of view of the manager (Figure 3) and the other from the point of view of the user (Figure 4).

The user does not have access to the information viewed by the manager, however, the manager has a complete view of the system. The basic idea is that though the various teams that are linked, each user has a different view of the system.
Information from the previously mentioned CVCS and CVE databases will be used to populate the internal database, creating a base of vulnerabilities referred to here as Risk. This information will be cross-checked with the software and hardware data obtained regarding the internal system, creating the basic contents, which include the IP address of the network machine, installed versions of softwares, information about the registered users, type of operating system, and hardware specifications (memory, processor, hard drive, etc.). The database created from the internal information collected is termed Inventory.

Figure 5 demonstrates the links between the different pieces of information obtained, with the CVSS and CVS updates being maintained by external organizations. The base Inventory and Central Repository are maintained by the client company. In order for the system to be efficient, all of the machines within the domain should have the inventory software installed (sensor) so as to continuously feed the internal database.

The company should have an established use policy. If none exists, the company should at minimum draw up “norms of usage of resources” by all users within the company. Normatives should contain information regarding:

- The installation and downloading of software, prohibiting users to install any software that is not company approved. This will also avoid the installation of unlicensed software.
- Terms of responsibility of use of company technological resources, explaining that their use must be work-related.
- Definition of limits of use of mobile resources (laptops, PDAs, etc.), prohibiting the use of non–company equipment.
- Installation of new technological resources such that any new equipment must contain the required software and must be inventoried.
- Creation of a login procedure for network users, so that only technological resources that have been inventoried will have access to the local network.
- The development of a dissemination policy so that all employees will be aware of company policies.

**A Risk Score Adequation**

Once all inventory information has been obtained, it is necessary to qualify each component regarding its importance. This qualification can be conducted by means of a questionnaire that should be completed by managers. In this manner,
the company obtains information regarding the machines/servers that would have greatest impact if they were compromised, in terms of physical or logistical problems. The flow diagram in Figure 6 summarizes the necessary data collection steps for risk analysis from this point forward.

The framework described above will be applicable for the following uses:

1. Correct identification of all assets and determination of their value as well as how critical each is for the company.
2. Estimation of the probability of the occurrence of a threat and calculation of the costs that would be involved if it should occur.
3. Identification of vulnerable points and development of protocols to minimize or contain the risk.
4. Creation of a strategy to minimize risks.

**B. Framework demonstration**

The proposed tool was developed utilizing JAVA programming language, with client/server support, where the server permits the visualization through a web server HTTP protocol. Initial tests utilized approximately 20 computers, with installed sensor information sent to a central repository.

The information obtained should be displayed or available in a consolidated manner, facilitating the identification of an actual risk resulting from a vulnerability, or permitting the visualization of the entire situation. The various vulnerabilities that have been identified should be assigned
to a specific team, initially responsible only for a specific product. Each team may ultimately be responsible for more than one inventoried product. Figure 7 shows a view of the system as seen by the manager. This comprehensive view is only seen by framework managers; framework users have a similar view limited to the products they support (see Figure 9).

Figure 7. Framework manager’s perspective of the system.

The system is monitored from the point of view of vulnerabilities (the number of vulnerabilities and the number of products affected). The framework provides managers with a high level view of products with vulnerabilities and teams that need more attention. Detailed information from teams and/or products can be obtained by managers by selecting the desired team/product (see Figures 8 and 9). Risk is measured based on the CVSS score as graphically illustrated in the pie charts by the colors red, yellow and green. At the moment a framework manager or user takes an action, this action is and must be registered (Figure 8) as part of the history of actions taken to resolve the problem. This facilitates future work as it establishes a minimum base of knowledge of procedures already attempted, making it easier to assign and distribute tasks, and thus making the process user independent and auditable.

The historical record keeps a log of the dates, actions taken and identities of the persons who executed the actions. This makes it possible to alter or adjust the vulnerability, through analysis or through laboratory work. It is also important to note that the status of the vulnerability situation can be “open”, “in the laboratory” or “under analysis”.

Figure 6. Procedures for Risk Analysis in the context of the proposed framework.
Once the vulnerability has been addressed, it is removed from the view. It has been demonstrated previously that even in empirical situations, the mere use of an available correction could result in even greater problems. For this reason, it is recommended that any changes or alterations be tested first in a laboratory situation and only then implemented in a production environment.

The access to information and the view of the system from the perspective of a specific framework user is limited to the view of his or her own team. Framework users do not have access to information that belongs to other teams (Figure 9). For this reason, the vulnerabilities pie graph is continuous, as the user is associated only with his/her own team. Meanwhile, the Products graph is associated with all products that may require intervention and that have had their vulnerabilities inventoried.

CVSS is also used to calculate risk. The user can find up to date information by simply clicking on the section of interest. All system vulnerabilities that have been inventoried can be seen (Figure 10), and can be further listed as “open”, “under analysis” or “in laboratory”, simplifying the follow-up response to pending resolutions. Additionally, deadlines can also be viewed so that, if a correction is made after a given deadline, it is possible to investigate the reason for the delay. The CVE can also be consulted directly for information about the CVSS score, the CVSS vector, general risk, brief descriptions, affected products, references, and the date on which the vulnerability was identified, published or modified.
In order for the system to function in an automated manner, each team must be defined (Figure 11). Additionally, the products under their responsibility must be defined. Filters can be used to, for example, verify which teams are active.

**VII. Conclusions and future work**

The laws of various countries are being adapted and modified to increase the transparency of corporate operations so as to increase the trust of investors. Adherence to laws will result in greater gains related to the quality of company processes, increasing their competitiveness and consequently, resulting in greater profits. In recent years, much has been invested in the purchase of security equipment, with the use of systems that detect intrusions, antivirus software, firewalls, and anti-spam, among many others. But in reality, is it possible to evaluate if these investments were worth while? Much of the generated information is ignored or not considered seriously in the process of information management. It is with respect to this issue that risk management may be of help by consolidating all available information and, most importantly, making this information useful.

The framework proposed by this article depends on various factors. Firstly, managers must be convinced that investing in information security is economically worthwhile, given that in the corporate environment all return is of a financial nature. Secondly, the IT infra-structure must be clearly defined in order to facilitate measurement of the return on investment (ROI) and with it the elaboration of a plan of action for risk analysis aimed at mitigating risk.
The tools suggested by the current study should initially be of an informative nature, providing basic information to the information manager, and utilizing the basic rules of the art of war\textsuperscript{2}: if you know yourself, you will have a chance at victory; if you know yourself and your enemy, you will have victory; if you know neither yourself nor your enemy, defeat is certain. This idiom relates to the persistent war that is carried out in worldwide networks, where dishonest companies attempt to obtain information illegally to gain a competitive advantage. The “enemy” is any entity that can use illegally obtained information for their own benefit and to the detriment of competitors.

It is impossible to efficiently manage risk if it has not been initially identified as risk. In other words, risk is based on uncertainty – in the absence of uncertainty, risk does not exist. It is in this context that the present work has been developed, with an aim to reduce the variables associated with uncertainty and consequently to reduce risk. In this context we propose a framework to control technological risks based on distributed sensors and a centralized vulnerability repository. As new vulnerabilities are published in the CVSS or any configuration change is communicated in real time from sensors throughout the corporate environment, the framework automatically adjusts to the changes so as to identify new risks. Once identified, the framework assigns the vulnerability to the team responsible for the related product, allowing corporations to take immediate actions to eliminate or mitigate the associated risks. To our knowledge, a framework based on real time analysis of configuration changes and known vulnerabilities has not been published before.

Future work includes hardening of the tools developed and full scale deployment in the corporate environment. The authors are also investigating how far automation could go in testing and deploying patches and updates as alternatives to reduce dependency on manual testing. Consideration of how sensors could be used to identify suspicious behavior of end users, based on patterns of configuration changes, is also within the scope of future research.

\textsuperscript{2} Sun Tzu

![Figure 10. Follow-up of vulnerabilities.](image-url)
### Teams

<table>
<thead>
<tr>
<th>Teams</th>
<th>Response</th>
<th>Situation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUPPORT - Office</td>
<td>John</td>
<td>Active</td>
</tr>
<tr>
<td>SUPPORT - Linux</td>
<td>Mary</td>
<td>Active</td>
</tr>
<tr>
<td>SUPPORT - OS2</td>
<td>Paul</td>
<td>Disable</td>
</tr>
</tbody>
</table>

Figure 11. Management of teams.

### References:


P. R. L. Gondim was born in Rio de Janeiro - RJ, Brazil, on February 23, 1957. He graduated in Computer Engineering (1987) and received his Master Degree in Computing and Systems (1992) from Military Engineering Institute, Rio de Janeiro - RJ, Brazil. He obtained his doctor degree in telecommunications at Catholic University (PUC-Rio), Rio de Janeiro - RJ, Brazil, 1998. He directed master degree dissertations in Computer Science and Communications Networks. He is a professor at the Electrical Engineering Department, University of Brasilia, Brasilia - DF, Brazil. His research interests include Networks and Wireless Technologies, Information Security, Quality of Service and Interactive Digital Television.

Laerte Peotta de Melo holds a degree in Electrical, electronic Modality by University Mackenzie-SP (1996), specialization in computer networks security by Catholic University of Brasilia (2004) and pursuing a Master Degree in Electrical Engineering at the University of Brasilia. Currently is Senior Security Analyst in information technology - Banco do Brasil - working in the area of information security and computer forensic. Professor and researcher at Catholic University of Brasilia, post graduation in computer networks security. Experience in electrical engineering area, with emphasis in telecommunications systems, acting mainly in the following subjects: Information security, Risk assessment, computer networks security, combat to digital crime, Information technology governance, compliance and free software.