Defining Network Exposure Metrics in Security Risk Scoring Models

Eli Weintraub[1], Yuval Cohen[2]
Afeka Academic College of Engineering
School of Industrial Engineering
Tel Aviv, Israel

***Abstract*—Organizations are exposed to cyber-attacks on a regular basis. Managers in these organizations are using scoring systems to evaluate the risks of the attacks they are exposed to. Information security methodologies define three major security objectives: confidentiality, integrity and availability. This work is focused on defining new network exposure measures affecting the availability. According to existing security scoring models network exposure risks are assessed by assigning availability measures on an ordinal scale using users' subjective assessment. In this work quantitative objective measures are defined and presented, based on the specific organizational network, thus improving accuracy of the scores computed by the current security risk scoring models.**

Keywords*—Security; cyber-attack; risk scoring; vulnerability; exposure

I. INTRODUCTION

Various kinds of damages are caused to organizational computerized systems by anonymous hostile entities. Damage can range from stealing data, to changing software, or paralyzing websites [1]. Organizations' computers are exposed to attacks for long periods of time, sometimes for weeks, from the moment a vulnerability has been detected until the time a patch is prepared. According to [2] there is a need for a solution that can rapidly evaluate system damages after cyber-attacks for recovery purposes of their information system. Evaluation of potential damages is important for configuration management planning decisions. Information systems contain large amounts of software components which might contain vulnerabilities stemming from logical planning or programming bugs. Attackers plan their attacks on components having specific vulnerabilities using exploits. Organizations are exposed to damages of three kinds named 'CIA triad": Loss of Confidentiality, Integrity and Availability. Organizations wishing to defend their network should have accurate knowledge of their network, focusing on systems' vulnerabilities. This article focuses on using accurate knowledge of computers' components' characteristics and networks' configuration. Defense strategy and execution is effective only if it considers the amount of potential damage and the vulnerability characteristics [3]. Risk is defined in literature as "An event where the outcome is uncertain" [4]. The approach leading this research is lessening the uncertainty by proposing quantitative objective metrics instead of qualitative subjective assessment of organizational risk managers.

This work focuses on risks to systems' availability. There are several definitions for availability. We use the definition of [5]: Availability is the capability of an information system to make information available including all the logical and physical resources and accessible whenever they are needed. Availability is usually evaluated using the MTBF and MTTF measures. Unavailability is used to measure the percentage of components that could be impacted by an attack on systems' components. Availability is the complement to 1 of that percentage. Current security risk models use an ordinal scale of three availability measures: High, Low and No impacts on availability, assigned by organizations' users. In this work availability measures are assigned real numbers in the range [0..1]. The greater the proportion of vulnerable components is the higher is the risk.

This work proposes a new measure called 'network availability exposure', which has not been considered, so far, in current security risk scoring models. Network Availability Exposure reflects the structure and characteristics of the software/hardware components of the network and the interrelationships between the components, which contribute to achieving good / bad network availability. For example, a network containing many vulnerable software components is exposed to external attackers exploiting the vulnerable components. Literature does not define any specific measure, nor scale for calculating the exposure of systems' network configuration to attacks. The proposed measure presented in this paper is based on the real-time information of systems' configuration, as proposed by [6].

This work focuses on measuring networks' availability exposure by quantifying the impacts of cyber-attacks on network components. The quantification is based on formulas developed for this purpose. According to the proposed model, each time a new vulnerability is published or when its status is updated, the metric is calculated and risk scores are re-evaluated. Developing new accurate assessments of risk scores is critical for planning organizations' risk management activities. Risk scores based on qualitative (subjective) estimates (which are currently been used) are prone to errors, and may cause organizations to under-estimate or over-estimate the risk. This in turn may lead to under-mitigation in situations of major risks, or over-mitigation investments in cases of minor risks. By using quantitative accurate risk measures, organizations will be able to build IT configurations in proportion to the risk. According to [7] the secure management of information under the conditions of frequent

changes is a complex recognized problem, but the common solution is still absent. This work defines new metrics based on the real-time network configuration and on the updated vulnerabilities of networks' components. The proposed metrics are based on three grounds: First, metrics are based on the knowledge concerning the characteristics of the attacked component within the actual configuration of the system. Second, risk calculations take into consideration the published history of actual vulnerabilities of the specific component. Third, the metrics are defined on a standard scale assigning quantitative, enabling comparisons to other networks' or other internal or external configurations.

The rest of the paper is organized as follows: Section II describes current known existing solutions. Section III presents network exposure metrics and computations. Section IV presents an illustration example. Section V concludes and suggests future research directions.

II. Existing Solutions

External vulnerabilities databases are used by security risk scoring systems for evaluating the risks organizations are facing. There are several owners of vulnerability databases [1]. Two popular systems are the Sans Internet Storm Center services and The National Vulnerability Database (NVD). Risk scoring systems make use of various parameters for estimating vulnerabilities' impacts on the target organization. Risk scores are evaluated through running a scoring algorithm while using the parameters for predicting potential attacks' damages. The Common Vulnerability Scoring System (CVSS) enables characterizing vulnerabilities and predicting risks by IT risk management professionals and researchers [1].

CVSS uses three groups of parameters: basic, temporal and environmental. Each group is represented by score compound parameters used for scoring computations. Basic parameters represent the intrinsic characteristics of the vulnerability, temporal parameters represent the vulnerabilities' specifications that might change over time due to defense activities taken. Environmental parameters represent the characteristics of vulnerabilities as configured by the specific organization, considering potential damages to that organization when exploits are being used by attackers. Basic and temporal parameters are specified by products' vendors who have the best knowledge of their product. Environmental parameters are specified by the users who have the best knowledge of their environments and attacks' impacts on their organization.

For Availability Impact (AI) evaluation CVSS uses three parameters: two base parameters 'Scope' and 'Availability', and one environmental parameter 'Availability Requirements'. Scope refers to the ability for a vulnerability in one component to impact resources beyond its privileges, assigned values 'unchanged' or 'changed'. Availability parameter measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. Availability Requirement environmental parameter is assigned values 'high', 'medium' or 'low'. Environmental parameters include three groups of parameters indicating security importance measures in the organization: 'Confidentiality Requirement', 'Integrity Requirements' and 'Availability Requirements'. 'Availability Requirement' represents the damage to the availability of the system in case of a successful attack on a component. Thus, no environmental parameter exists for measuring networks' exposure – which is the focus of this work. The environmental group of parameters enables to customize the CVSS score depending on the importance of the impacted IT asset to a user's organization. The full effect on the overall risk score is determined by the scoring algorithm by incorporating the base impact metrics into the environmental metrics producing the overall security risk score. This work suggests adding the new environmental exposure impact measures into the computations of the availability measure. The availability measure is used for overall risk scoring computations.

All CVSS parameters are assigned ordinal qualitative values which are based on the knowledge of human experts. For example, the 'Availability Requirement' parameter is assigned values High, Medium, Low which do not differentiate between 0.99 availability and 0.999 availability, both are considered high. Also, organizations might assign a specific availability measure as high while other organizations might assign the same availability to medium. Parameter values are not based on the specific characteristics of the network. The new suggested exposure measure will be quantitative, in contrast to current metrics.

According to [8] unavailability is not an option in todays' echo systems, given the heavy dependence of modern organizations on information resources. Availability is the least discussed and researched security attribute, although it is not the least important attribute. In fact, it plays an important role in determining the other attributes of security (confidentiality and integrity). According to [5] availability measurements should take into consideration the logical and physical resources, to enable accessibility whenever the information is needed. In [8] describe the factors availability is dependent upon as software, hardware and network. A system might be exploited step by step by gaining access from the upper layers. Current models do not take into consideration those issues. The proposed model measures network exposure to the actual known vulnerabilities. The model considers networks' components exposure specifically and evaluates network exposure by considering components' interrelationships.

According to Federal Information Processing Standards (FIPS) 199.5 [9] organizations assign their IT resources importance measures based on component location, business function using it, and potential losses in case the component is damaged. For example, U.S. government assigns every IT asset to a group of assets called a system. Every system must be assigned three "potential impact" ratings according to three security objectives to represent the potential impact on the organization in case the system is compromised. Thus, every IT asset in the U.S. government has a potential impact rating with respect to security objectives. CVSS follows this general model but does not require organizations to use specific tools for assigning the impact ratings. In [10], author states that organizations should define the specifications of security risks of their specific environment. The Department of State has implemented a scoring program called iPost that is intended to

provide continuous monitoring capabilities of information security risks for IT infrastructure. According to [11], the iPOST scoring model does not define the base scores of CVSS to reflect the characteristics of its specific environment. This work presents a model aimed to close this gap.

Quantification of the environmental parameters in CVSS algorithm has been recently presented in a research demonstrating improvements in accuracy of risk scores by using the actual IT configuration [12]; Incorporating the information relating to the actual IT components into the scoring algorithm metrics changes the risk scores to be objective rather than subjective measures [13]. Moreover, components' specifications are expressed in high resolution of the smallest IT elements rather than an overall configurational metric which shades smaller components' characteristics. Risks quantification is based on a configuration management database system (CMDB) which makes use of systems' metadata on the elementary components and their interrelationships according to security specifications (ibid). This paper continues the same line of research, aimed at improving risk scoring accuracy in relation to existing risk scoring models such as CVSS, by adding a quantitative metric rather than an ordinal subjective assessment and basing evaluations on the specific organizations' configuration.

III. Network Exposure Metrics and Computations

The proposed approach produces estimates to the risk of losing availability, meaning the risk of system malfunction or system failure. It gives both overall network measures, as well as risk measures for single components. An information system is consisted of one computer operating many hardware /software components, or a communication network consisting of many computers communicating between each other. The network is represented as a graph, components are represented by nodes. Links between nodes represent information passing between the connected nodes. Components represent hardware or software entities. Some definitions are now in order to be used for further developments.

A. Definitions

Diameter – Minimal number of links between two points defined on the edge of the network or subnetwork.

Working nodes – Uncompromised nodes

Impacted nodes – Compromised nodes

Impacted link – A link having at least one compromised node.

M – Total number of impacted nodes

m – Number of impacted nodes having at least 2 neighboring impacted nodes

d - Maximal diameter of the network generated by the impacted (compromised) nodes

*D' – M*aximal total network diameter

D – Degree = Number of links emanating from a node

Dir – Number of impacted links emanating from a node

Sec - Number of links to risky nodes, which are still working but have direct links to impacted nodes.

W – The number of arcs connected to working nodes

For the reader's convenience we shortly repeat the definitions in the proposed availability measures. In case, where the organizational network is attacked the following three network measures are suggested.

1) **Damage%:** Percentage of nodes impacted: range of values is [0 to 1]. This measure represents the damage to the whole network, calculated by computing the percentage of impacted nodes out of all nodes.

2) **Dispersion:** The ratio *d/*D' between *d*=maximal diameter of the impacted nodes, and *D'*=maximal total network diameter: range of values is [0 to 1]. *D'* the number of links in the maximal shortest path that connects between each pair of nodes; and *d* is the number of links in the maximal shortest path that connects between each pair of un-impacted neighbors of the impacted nodes.

3) **Concentration:** The ratio of *m/M* between *m*= number of impacted nodes with at least 2 neighboring impacted nodes, and *M*=total number of impacted nodes. Range of values is [0 to 1]. The measure represents the proportion of the seriously impacted nodes. A concentration of disconnected nodes signifies the severity of the impacts on systems' availability. possibly leading to situations of paralyzing the impacted area. Nodes connected to 2 or more impacted nodes might be disconnected more easily.

In case where the organization is a node in the larger network, and in cases of measuring the exposure of a specific node in an organizational network, the following three node risk measures are proposed:

1) **Directs**: defined as *Dir/D*; where *D* is the node degree (number of arcs emanating from it), and *Dir* is the number of impacted direct links: range of values is [0 to 1]. This measure represents the proportion of the directly impacted links between the node and its' neighboring nodes.

2) **Seconds:** defined as *Sec/D* where *D* is the node degree (number of arcs emanating from it), and ***Sec*** is the number of links to working nodes having direct links to impacted nodes. The Seconds range of values is [0 to 1]. The measure represents the proportion of links to working nodes which have direct links to other impacted nodes. Those working nodes are exposed now to risks in cases of a second forthcoming attack coming from an already attacked component, thus, leading to a direct attack on the subject component.

3) **Disconnection risk**: defined as (1/*W*), where *W* is the number of arcs connected to working nodes (with the exception that when this number is zero (disconnection), *W*=1). Thus, when only one arc is connected to a working node *Disconnection risk* =1; and when all arcs are connected to working nodes, the *Disconnection risk* =1/*D* (where *D* is the node degree). The measure represents the efforts needed by an attacker who wishes to disconnect a node. The proportion

means he needs to disconnect W links. As W is higher the effort are higher and the organizations' disconnection risk is smaller.

IV. Illustration Example

The following case study illustrates the suggested measures, their computations, their meaning and effectiveness and their importance. Fig. 1 describes an example network with 20 computerized nodes after a first wave of attacks which culminated with failures of nodes 14, 16, and 17.

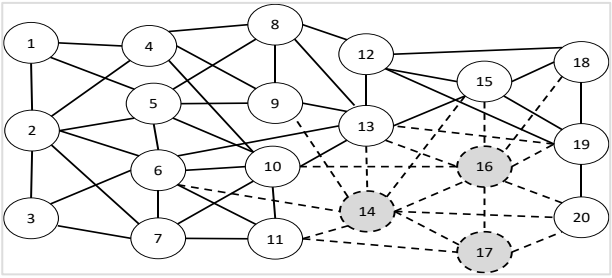

Fig. 1. Computer Nodes Network after attack wave – 1.

The 20 computer nodes network example with 3 impacted nodes (denoted by grey and dashed lines) and dashed lines are disconnected communication lines due to the hackers' attack.

In Fig. 1 the network exposure measures are:

1) **Damage %:** Percentage of nodes impacted: 3/20= 0.15.

2) **Dispersion**: The ratio *d/D'* =3/5 = 0.6. Where *d* the diameter of the impacted nodes: **3**, and ***D'*** the network diameter is *5*.

3) **Concentration**: The ratio of *m/M* = 3/3 = 1 the number of impacted nodes: **3** each is connected to the other two.

To illustrate the node measures for Fig. 1, we chose to compute measures for nodes: 20, 15, 9, 6, 3. For brevity purpose we shall use: "Directs" for directly impacted neighbors, "Seconds" for second degree impacted neighbors, and "Arcs" for the degree of the non-impacted node.

For node 20: *Directs* = 3/4, *Seconds* = 1/4 (node 19 "Directs">0), *Disconnection risk* =1/1=1

For node **15**: *Directs* = 2/6, *Seconds* = 3/6 (13, 18, 19 have "Directs">0), *Disconnection risk* =1/4

For node **9**: *Directs* = 1/5, *Seconds* = 1/5 (node 13 have "Directs">0), *Disconnection risk* =1/4

For node **6**: *Directs* = 1/8, *Seconds* = 3/8 (10, 11, 13 have "Directs">0), *Disconnection risk* =1/7

For node **3**: *Directs* =0, *Seconds* = 0, *Disconnection risk* =1/3

It follows that immediate risk is highest for node 20 with *Directs*=3/4 (followed by node 15), while risk evolution potential is highest for nodes 15 and 6 with *Seconds*=3/6, and 3/8, respectively, and disconnection risk is highest for node 20 (*Disconnection risk* =1).

The example follows with hacker attack evolution as depicted in Fig. 2.

Fig. 2 illustrates the example network with 20 computerized nodes after a second wave of attacks which culminated with failures of nodes 9, 13, 19 (in addition to previously failed nodes: 14, 16, and 17).

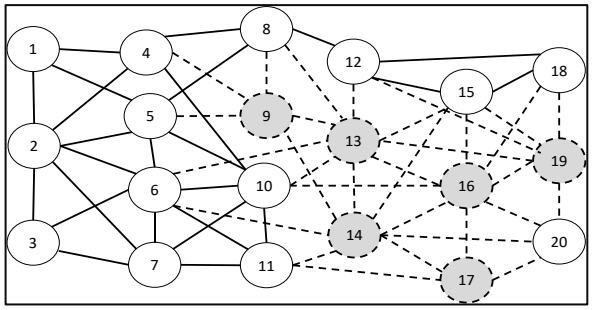

Fig. 2. Computer Nodes Network after attack wave – 2.

The 20 computer nodes network example with 6 impacted nodes (denoted by grey and dashed lines - dashed lines are disconnected communication lines due to the hackers' attack).

In Fig. 2, the network exposure measures are:

1) **Damage %**: 6/20= 0.3 twice the number in Fig. 1.

2) **Dispersion**: The diameter of the impacted nodes: 4/5 (the number of links in the maximal path that connects minimally between each pair of un-impacted neighbors of the impacted nodes) for example: 20-16-13-9-4. Diameter of 4 is an increase from 3 in Fig. 1.

3) **Concentration:** The largest connected group of at least two neighboring impacted nodes = **6** which is as large as the number of impacted nodes=6. So: 6/6=1.

To illustrate the node measures for Fig. 2, we compute measures for nodes: 20, 15, 9, 6, 3. These could be easily compared to the measures for Fig. 1.

For node 20: *Directs* = 4/4, *Seconds* = 0, *Disconnection risk* =1 (disconnected)

For node **15**: *Directs* = 4/6, *Seconds* = 2/6 (12, 18 have "Directs">0), *Disconnection risk* =1/2

For node **9**: Impacted.

For node **6**: *Directs* = 2/8, *Seconds* = 3/8 (5, 10, 11, have "Directs">0), *Disconnection risk* =1/6

For node **3**: *Directs* =0, *Seconds* = 1/3 (node 6 have "Directs">0), *Disconnection risk* =1/3

Thus, node 9 failed, node 20 is disconnected (*Disconnection risk* =1), node 15 faces high immediate and intermediate risk along with disconnection risk. Node 6 has immediate and intermediate risk exposure, but its disconnection is unlikely (*Disconnection risk* =1/6). Finally, node 3 has small intermediate risk exposure (Seconds=1/3).

- Attack Evolution Analysis

Table I summarizes the node exposure metrics evolution along two waves attack. Analyzing node exposure evolution might help decision makers in planning their network mitigation activities. Looking at to Directs column might lead

to decision of defending node 15 which has the highest direct-damage measure. Looking at the secondary-damage probability might lead to defending node 15 with highest measure, but in case we have already decided to defend it, we might decide now to defend node 6. Looking at the disconnection column leads to the understanding that it would be reasonable to defend node 15, but if we have already defended it then we will defend node 3.

TABLE I. ATTACK EVOLUTION: 2-WAVES EXAMPLE

Node/wave	Direct impact	Secondary impact	Disconnection
20 1	**0.75**	**0.25**	1
2	**1**	**0**	1
15 1	**0.33**	0.50	**0.25**
2	**0.67**	0.33	**0.50**
9 1	0.20	0.20	0.25
2	**impacted**		
6 1	**0.125**	0.375	**0.14**
2	**0.25**	0.125	**0.17**
3 1	0	**0**	0.33
2	0	**0.33**	0.33

These measures help decision makers in prevention planning activities. For example, node 20 would be very interested in adding a link to node 15, or 12.

Moreover, the new measures could help in restoration priorities. The impacts of restoring alternative nodes could now be simulated. For example, suppose that the resources for restoration are limited to one node at a time. Comparing alternatives would be an efficient decision support tool. For example, in Fig. 2: comparing restoration of node 16 to node 17 yields the following measures, referring to Fig. 2. A single restoration would change the number of impacted nodes from 6 to 5 and the impacts on network measures are relatively small:

For restoring node 16 – network measures: Damage % =5/20; Dispersion=4/5; Concentration=4/6

For restoring node 17– network measures: Damage %=5/20; Dispersion=4/5; Concentration=5/6.

Thus, analyzing network exposure measures leads to a decision to restore node 16.

Let's see now the impacts on the neighboring nodes.

The impact of restoration is always on specific neighboring nodes. So, for restoring node 16 vs. 17: the neighboring node of 16 and 17 are nodes 20 and 15. The measures for node 20 are the same, but for node 15 the measures are in favor of 16.

For node 20: *Directs* = 3/4, vs. 3/4, *Seconds* = 1 vs. 1, *Disconnection risk* =1 vs. 1

For node 15: *Directs* = 3/6, vs. 4/6, *Seconds* = 3/6 vs 2/6 (12, 18 have "Directs">0), *Disconnection risk* =1/3 vs. 1/2

Thus, restoring node 16 (vs. restoring node 17) has smaller direct risk, higher secondary risk, but more arcs meaning less disconnection risk.

Thus, after analyzing both, network exposure and node measures, it may be concluded that restoring node 16 has a priority over node 17.

The standpoint of the authors of this paper stress that current risk scoring models should be enhanced regarding all security objectives. The enhancements should be implemented taking several phases: First, incorporating the real configurations' characteristics into the scoring model. Secondly, transforming all the parameters defined as inputs to the scoring model as quantitative measures reflecting the actual organization environment rather than ordinal subjective users' assessments. Thirdly, scoring models should define new metrics expressing all risk objectives, relating to a whole environment rather than a specific component. The models should define the characteristics of a whole network and all interrelationships between the network and each of its internal components. Current scoring models do not support modeling the characteristics of the whole network, as has been shown in this research, dealing with the availability security measure. This is just one first example. The fourth phase should include metrics considering the time dimension such as this paper suggests: measuring the development of damages caused to a network as a continuous attack spreading in the different zones of the network. Such time-related measures should incorporate more complex graph-theory models and prediction algorithms looking at the historical network changes.

V. CONCLUSIONS

This work presents a risk assessment model with a focus on new availability risk measures, measuring the network security and node security, as part of an overall risk assessment. According to the proposed model, CVSS will use the new network exposure environmental parameters which are evaluated using a new formula based on the configuration of the system. The new measures are quantitative, normalized to [0..1] and based on the actual networks' configuration. This is contrary to the existing models which do not measure the impacts of network exposure on the overall risk, but consider networks' configuration implicitly relying on intuitive users' subjective assessment.

Regarding the practical use of the theoretic results, the model helps risk managers in assessing the damages caused to firms' components in occasions of cyber-attacks. Using the proposed model will enable predicting accurate measures of organizational damages taking in consideration components' actual characteristics and the availability exposure of the network as an integrated entity. The suggested model enables efficient risk mitigation planning and improved defense to organizations. Risk managers will be able to assign risk budgets according to accurate and actual risk measures, thus focusing on the high-priority risks, and preventing unnecessary budgets to low-order risks.

The new network exposure metrics enable customizing the CVSS score to the characteristics of the attacked IT asset, its interrelationships to other assets, and the exposure characteristics of the network on the damages to user's organization. According to the proposed model, a formula which assigns quantitative measures to exposures' impacts based on the actual updated vulnerabilities of the specific component. The proposed model outlines the structure of a CMS which uses the real organizational environment and components, and the processes which update the network exposure parameters with the planned and actual values. The framework enables getting accurate risk measures, thus enabling the organization making better risk management decisions, allocating risk management budgets in proportion to the risks.

Limitations of the study are related to two issues: First is the feasibility of a managing a graph describing the real-time status of each component and its interrelationships to other components, including all security characteristics. Such a graph might be difficult to update at every attack or configuration-change. Second limitation refers to the various connections possible between two nodes. It is reasonable to assume that not all connections enable transferring the cyber-attack to other nodes. It is possible to assume that there are connection-types that do not transfer the attacker to other connected nodes. This issue is a limitation of the current model and also a research issue.

Further research directions are:

- Designing ways of incorporating the new availability metrics in CVSS framework.
- Algorithm formalization including complexity measures calculations.
- Using more expressive graph models to represent varying node-types and varying connections among network nodes. It is reasonable to assume that certain connections may have more impact on the damages caused to neighboring nodes.
- Further development of the algorithm to calculate N-wave metrics and measures predictions of the N value at which the whole network will be paralyzed.
- Research aimed at predicting attack evolution for decisions concerning mitigation activities for the long run of future attacks.

Future improvements may focus on building a full dash-board of system exposure metrics from its component measures.

More research is needed in studying the impacts of the various proposed network exposure measures on the overall security risk score.

REFERENCES

[1] P. Mell, & K. Scarfone, & S. Romanosky, "CVSS – Common Vulnerability Scoring System v3.0: Specification Document", FIRST Org, 2015.

[2] Y.F. Nũez, "Maximizing an organizations' security posture by distributedly assessing and remeding system vulnerabilities", IEEE – International Conference on Networking, Sensing and Control, China, April 6-8, 2008.

[3] S. Tom, & D. Berrett, "Recommended practice for patch management of control systems", DHS National Cyber Security Division Control Systems Security Program, 2008.

[4] A. Terje, & R. Ortwin., "On risk defined as an event where the outcome is uncertain", Journal of Risk Research Vol. 12, 2009.

[5] D. Khazanchi, & A.P. Martin, Information Availability: Handbook of Research on Information Security and Assurance, 2008.

[6] E. Weintraub., "Security Risk Scoring Incorporating Computers' Environment", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7(4), April 2016.

[7] B. Carpenter, "The Internet Engineering Task Force. Overview, Activities, Priorities". IETF Report to ISOC BoT, Oct. 2006.

[8] S. Qadir, & S.M.K. Quadri, "Information Availability: An insight into the most important Attributes of Information security", Journal of Information Security, pp. 185-195, 2016.

[9] K. Dempsey, & N.S. Chawia, & A. Johnson, & R. Johnson, & A.C. Jones, & A. Orebaugh, & M. Scholl, & K. Stine, "Information security continuous monitoring (ISCM) for federal information systems and organizations", NIST, 2011.

[10] R. Sandhu, & D. Ferraiolo, & R. Kuhn, "The NIST Model for Role-Based Access Control: Towards A Unified Standard", George Mason Univ., 1999.

[11] A. Keller., & S. Subramanianm., "Best practices for deploying a CMDB in large-scale environments", Proceedings of the IFIP/IEEE International conference and Symposium on Integrated Network Management, pages 732-745, NJ, IEEE Press Piscataway, 2009.

[12] E. Weintraub, "Evaluating Damage Potential in Security Risk Scoring Models", International Journal of Advanced Computer Science and Applications (IJACSA), 7(5), 2016.

[13] E. Weintraub, Y.Cohen, "Security Risk Assessment of Cloud Computing Services in a Ne tworked Environment" International Journal of Advanced Computer Science and Applications (IJACSA), 7(11), 2016, 79-90.