Taxonomy of Information Security Risk Assessment (ISRA)

Alireza Shameli-Sendi[1], Rouzbeh Aghababaei-Barzegar[2], and Mohamed Cheriet[3]
[1]School of Computer Science, McGill University, Montreal, Canada
[2]Department of Information Security Framework Management, Ernst & Young GmbH, Frankfurt, Germany
[3]Ecole de Technologie Superieure (ETS), University of Quebec, Montreal, Canada
alireza.shameli-sendi@cs.mcgill.ca, rouzbeh.a.barzegar@de.ey.com, mohamed.cheriet@etsmtl.ca

***Abstract*—Information is a perennially significant business asset in all organizations. Therefore, it must be protected as any other valuable asset. This is the objective of information security, and an information security program provides this kind of protection for a company's information assets and for the company as a whole. One of the best ways to address information security problems in the corporate world is through a risk-based approach. In this paper, we present a taxonomy of security risk assessment drawn from 125 papers published from 1995 to May 2014. Organizations with different size may face problems in selecting suitable risk assessment methods that satisfy their needs. Although many risk-based approaches have been proposed, most of them are based on the old taxonomy, avoiding the need for considering and applying the important criteria in assessing risk raised by rapidly changing technologies and the attackers knowledge level. In this paper, we discuss the key features of risk assessment that should be included in an information security management system. We believe that our new risk assessment taxonomy helps organizations to not only understand the risk assessment better by comparing different new concepts but also select a suitable way to conduct the risk assessment properly. Moreover, this taxonomy will open up interesting avenues for future research in the growing field of security risk assessment.**

***Index Terms*—Information security, Risk assessment, Risk management, Risk analysis, Threat, Vulnerability.**

I. Introduction

Information is a perennially important business asset, and needs to be protected like any other valuable asset [1], [2]. The value of information assets varies from one organization to another not only with the type and size of the business, but also on the role of those assets in delivering particular services [36]. Especially because of its relatively important role in surviving in today's increasingly competitive marketplace, data are rapidly becoming the focus of business executives [3]. According to the Ponemon Institute's report, the average cost of a data breach in the UK increased by 68% from £47 in 2007 to £79 in 2011 [7]. This sharp increase could be considered as a sign that the value of information to organizations is growing dramatically. However, for some kinds of information, like medical records, where a single loss could be a matter of life or death, its value cannot be measured in terms of monetary value alone [8].

In Kaspersky Lab's Global IT Risk Survey, 50% of the respondents ranked cyber threats as a leading business threat, next to economic uncertainty [28]. These threats and the corresponding risks are generated by hackers, malicious software, disgruntled employees, competitors, and other sources, all of which are called threat agents. The agents can be either internal or external to an organization, and have a diversity of interests and motivations [4], [12]. According to Verizon's Data Breach Investigations Report, 96% of security breaches in 2012 were motivated by financial or personal gain [29]. The same report shows that 79% of the victims were targets of opportunity, attacked only because they had an easily exploitable vulnerability, and 96% of all attacks were not considered to be difficult to perpetrate. These are the facts that have attracted the attention of researchers, professionals, journalists, legislators, governments, and even ordinary citizens to information security and its practices [19].

One of the best ways to approach information security problems in the corporate world is to take a

risk-based approach [17], [63]. With the widespread use of IT, and the ever increasing dependency of organizations' on it, businesses may not only have to avoid risks but manage them properly as well [37]. Information security risk management is a continuous process which gives businesses an understanding of the potential risks to the organization's valuable information assets and the tools to address them [12], [14], [38]. When it comes to real world implementation, information security risk management is a challenging process, because unlike in hypothetical scenarios, the risk factors are constantly changing. Even if precise information is also provided, due to rapidly changing technologies and the attackers knowledge level, we cannot be satisfied even with the recent months results. Moreover, the judgments of the individuals should be integrated and analyzed comprehensively in the organization [24], [37], [74].

Information security risk assessment (ISRA) is a major part of an Information Security Management System (ISMS) which enables an organization to identify vulnerabilities and threats, and then to decide which countermeasures to choose to address potential threats [12], [21]. Moreover, those threats are becoming increasingly sophisticated, and more resources than ever before are required to neutralize them, and this at a time when information security budgets are shrinking [17]. As a result, management in charge of information security tends to perform a rather "ruthless triage", to ensure that their scarce resources are assigned to the risks with the highest priority and to protect themselves in a cost-effective way [10], [18], [19], [54], [78]. Organizations which do not conduct risk assessment properly and regularly may experience severe consequences, like loss of reputation, legal issues, or even a direct financial impact [23].

A number of ISRA approaches have been developed, like NIST SP 800-30 [34]; ISO/IEC 27005 [72]; CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method) [47]; Microsoft's Risk Assessment model [51]; the Facilitated Risk Assessment Process (FRAP) [55]; Consultative, Objective and Bifunctional Risk Analysis (COBRA); CORAS [48]; and the Operationally Critical Threat and Vulnerability Evaluation (OCTAVE) [49], which can be applied in all types of organizations [23], [25]. But, despite the variety of these approaches, there are some business requirements that none of them can meet [22]. The problem with many of these methodologies is that they concentrate mainly on general principles and guidelines, leaving users without adequate details for implementation [26]. Even industry standards, like COBIT (Control Objectives for Information and Related Technology) [62] and ISO/IEC 27002 [2], fail to provide managers with a clear and simple visualization of the security risk assessment and leave the operational details untouched [27].

In this paper, we will introduce a new taxonomy for information security risk assessment approaches which will remove many ambiguities created by the previous one [9], [51], [56], [93]. The previous widely accepted taxonomy classifies ISRA approaches based on three criteria: *Quantitative*, *Qualitative*, and *Hybrid (Semi-Quantitative)*. This old taxonomy only differentiates between ISRA approaches based on their method in assigning numerical values or classes/relative values to resources (i.e. assets, services, or business processes), vulnerabilities, and threats. It could not answer the following questions to classify the ISRA approaches: 1) Which level of abstraction is considered for ISRA: assets, services, or business processes? 2) How is the resource value calculated? 3) Are the relationships between resources considered in resource valuation process or not? 4) Is the propagation of attack impact from the compromised resource considered in all dependent resources, in risk evaluation process, or not? 5) How many kinds of attack impact propagation can be distinguished from the compromised resource?.

The previous taxonomy is considered as one element of our new proposed taxonomy. We classify the existing approaches to information security risk assessment, with the goal of providing a comprehensive survey of these methods and identifying their strengths and weaknesses. We believe that this survey and study of risk assessment methods are important, in that it will help explain the critical issues involved and lead to the development of more comprehensive and effective risk assessment mechanisms. It may also help organizations to find the most appropriate approach for their risk assess-

ment or even develop their own on the basis of the available approaches.

The rest of this paper is organized as follows: In Section II, the boundaries and scope of the survey are introduced, and a methodology to extract the literature is illustrated. In Section III, main concepts of information security and risk management process are defined. In Section IV, we present our information security risk assessment taxonomy. Section V provides an overview of the research and development of information security risk assessment approaches. In Section VI, we discuss the weaknesses, problems, and constraints of current approaches. Finally, in Section VII, we present our conclusions.

II. Scope and Assumptions of the Survey

A. Inclusion and Exclusion Criteria

A total of 125 papers from 1995 to May 2014 were obtained and reviewed. Papers were found via computerized search of the information security risk assessment. The papers were searched according to the online databases: Science Direct, IEEE Xplore, Springer Link Online Libraries, ACM Digital Library, Wiley InterScience, and Ingenta Journals. The papers were carefully reviewed to select those that considered ISRA as the core part. Because of the nature and importance of information security risk assessment concepts, mainly three kinds of references are used in this survey: academic references (conference papers, journal papers, masters and doctoral dissertations), international/national standards, and books. International standards are used because they form the main guidelines in this area in all industries all over the world and non-conformity with these standards may cause many hard and soft impacts for the organizations and impose them to another risks. On the other hand, books are used because the main concepts need deeper and wider explanation than those which could be found in academic papers. The only exam material used in this paper is "CISSP All-in-One Exam Guide" which is chosen because of the importance of this certification (CISSP) in information security [4]. This way, we tried to unite academic and industrial aspects of ISRA together in our paper. Other publication forms such as magazines or newspapers were not included.

B. Methodology

The objective of risk assessment is to identify all possible risks to the assets and evaluate them accurately to mitigate risks appropriately. Thus, the vulnerabilities of each valuable resource (i.e. asset, service, business process) and the threats that might take advantage of them are identified and then the relationship between vulnerability and threat is defined as a risk. Based on a very old taxonomy, the current information security risk assessment approaches are classified based on three criteria: *Quantitative*, *Qualitative*, and *Hybrid (Semi-Quantitative)* [9], [34], [51], [56], [93]. The primary focus of this taxonomy (C_1), which we prefer to call *Appraisement*, is on the type of input and output of risk calculation. In other words, it only differentiates between ISRA approaches based on their method in assigning numerical values or classes/relative values to resources, vulnerabilities, and threats. Besides this category (C_1), we have reached three other categories presented in this paper:

- **Perspective** (C_2): Our first new category is about the perspective adopted by an ISRA approach in risk identification and assessment. If we consider the three levels of bottom-up abstractions - asset, service, and business process - researchers can look at the information security risks in different levels. Although the majority of approaches lie in asset level, the new studies are changing the angle, and they believe that working on the service level or business process level is easier and more accurate [77], [81].
- **Resource Valuation** (C_3): The second new category is related to resource valuation model. The accurate model can segregate the critical and non-critical resources, and leads us to an efficient ISRA. If we consider the three levels of bottom-up abstractions - asset, service, and business process - some papers have considered the functional dependency between levels to figure out which resource has the critical role in the organization [79], [80]. Some other studies believe that the resource dependency model should be considered in the resource level as well to reach a comprehensive model for valuing resources [68], [69].

- **Risk Measurement** (C_4): The third new category refers to the risk measurement part. Some studies believe that the impact of the attack on a resource is usually propagated to other resources, and we should consider the risk propagation to have a better picture of the damage cost [67], [86], [89].

The new categories (C_2, C_3, and C_4) are found in comprehensive studying, and we do not see any other category in risk assessment at this moment. As Table I illustrates and will be discussed in Section V, we completely covered all studies that fit in classifications C_2, C_3, and C_4.

III. Information Security Risk Management

Holton [32] defines risk as the exposure to any proposition which involves uncertainty. By definition, information security is the protection of an organization's valuable information from unwanted exposure, tampering, or destruction [20]. The ultimate goal of an information security program based on risk management is to maximize the organization's output (products or services), while at the same time minimizing the unexpected negative outcomes generated by potential risks [15], [39]. It is important that risks be managed in a way that gives confidence to all stakeholders [22], [30], and provides an appropriate level of security for the information systems that support the organization's ongoing operations [37]. With proper risk management, a balance between potential risks and acceptable risks can be achieved [35]. In other words, risk management processes should be repeatable, measureable, and auditable, and it should be possible to model them as well [22].

There are different types of information security risk management frameworks. Each of these frameworks has been developed to meet a particular need. Hence, they have different objectives and steps. In continuation, we provide a general view and structure of information security risk management. Risk management comprises four processes: *Framing risk*, *Assessing risk*, *Responding to risk*, and *Monitoring risk* [34].

A. Framing Risk

This is the first process in the information security risk management approach, and concerns how an organization views the risks it faces. The major output of this process is a risk management strategy, which also delineates the boundaries of risk management within the organization [5], [34]. Assets and resources that are known to be unimportant to the organization do not need to be assessed any further. Both underscoping and overscoping are dangerous practices in information security risk assessment, and can be avoided by carefully identifying the organization's critical assets [12].

B. Assessing Risk

Risk assessment is composed of risk analysis and risk evaluation [40]. It provides a systematic way for the organization to obtain a comprehensive view of existing information security risks and their consequences, and the countermeasures to deal with them [38]. Since assessment process includes the risks associated with all kinds of platforms, operating systems, application programs, networks, people, and processes, as well as the interdependencies between them, it is a challenging process, and, in most cases, organizations require outside help to perform it properly [8], [22]. Note that mistakes in risk assessment can be dangerous and costly. Underestimating the risks can leave the organization vulnerable to severe threats, whereas by overestimating them, some useful IT services and technologies might be withdrawn [16].

1) Risk Analysis: Risk analysis identifies the organization's valuable information assets and their vulnerabilities, reveals threats that may take advantage of those vulnerabilities and put the organization at some sort of risk, and, finally, estimates the possible damage and potential losses resulting from those risks [4]. We discuss the risk analysis steps in detail below:

(i) Resource Identification and Valuation: Identifying and evaluating information assets/resources is a critical first step in risk analysis. In general, information assets are either tangible or intangible, and are assets which are valuable to the organization [12]. ISO/IEC 27001 (Control number A.8.1.1) requires organizations to create and maintain an up-to-date inventory of information assets [40]. Examples

include business processes and activities, information, computer hardware and software, network, personnel, and documents, as well as the organization's brand and reputation [72]. These resources may have different values, and they must be identified based on their importance to the organization [15]. Londoll [12] defines four types of qualitative asset valuation appraisement:

1) Binary asset valuation
2) Classification-based asset valuation
3) Rank-based asset valuation
4) Consensus-based asset valuation

He also defines three quantitative asset valuation appraisements:

1) Cost valuation
2) Market valuation
3) Income valuation

(ii) Risk Identification: The objective of this step is to identify all possible risks to the assets. Thus, the vulnerabilities of each valuable resource and the threats that might take advantage of them are identified, and then the relationship between vulnerability and threat is defined as a risk. Vulnerabilities can be identified and assessed using the following methods, based on how critical the information assets are to the organization and the availability of resources [11], [15], [31], [72]:

- Automated vulnerability scanning tool
- Security testing and evaluation
- Penetration testing
- Code review

These methods may yield some false positives, and so the following activities may be considered [72]:

- On-site interviews
- Questionnaires
- Physical inspection
- Document review

Vulnerabilities can also be identified from the results of previous risk analysis, IT system audit reports, system anomaly reports, security review reports, and system test and evaluation reports. Other potential sources are vendor advisories and public vulnerability databases, like the National Vulnerability Database (NVD) [41].

Threats are identified and documented through a formal process called threat modeling. There are several methods available to identify threats to a system and map them with the related vulnerabilities [35]. ISO/IEC 7498-2 defines a reference model of major security threats [33]:

- Destruction of information and/or other resources
- Corruption or modification of information
- Theft, removal, or loss of information and/or other resources
- Disclosure of information
- Interruption of services

(iii) Risk Measurement: In this step, the organization needs to choose a model to measure risk. Risk model specifies the relationship among risk factors which include resource value, vulnerability effect, threat impact, threat likelihood, and so on [34]. Based on the chosen model, the risk value for each incident scenario is measured. In the process of risk assessment, it is also important to identify existing/planned safeguards. Failing to consider all of these safeguards will result in an inaccurate risk assessment report, which will generate unnecessary costs for the organization and also put the business in danger because of risk overestimation [12], [78].

2) Risk Evaluation: Risk evaluation is the process of rating risk exposures on a scale and against accepted risk criteria to determine the significance of each risk [40]. Then we need to determine the proper steps to take to manage the risks and address them appropriately [15]. In this phase, the identified risks need to be prioritized based on their relative probability of occurrence and their legal, regulatory, financial, or reputational impact to the organization in order to make decisions on their treatment [13], [22].

There are four ways to address a particular risk [4], [12], [15]:

- *Accept:* The organization understands the risk and its consequences and consciously decides to accept it.
- *Avoid:* The activity that is exposing the organization to one or more risks is avoided altogether.
- *Transfer:* All or part of the responsibilities and liabilities associated with a particular activity and the related risk are shifted to another party.
- *Mitigate:* The risk and its consequences are controlled and limited in some way, reducing

the risk to a level that is lower than the organization's acceptance level.

Usually, handling an organization's risks involves a combination of these ways: some of them are avoided, some are transferred, some are mitigated, and the rest are accepted [22]. As a part of the risk evaluation process and depending on the organization's policies, goals, and objectives, and the interests of stakeholders, the risk acceptance level (criteria) should be defined. All the risks under this level are accepted (tolerated) by the organization's management, but senior management has the right to accept risks above this level [72].

C. Responding to Risk

Information security risks which are above the risk acceptance level should be responded in any of the other mentioned ways of addressing risks, namely risk avoidance, transfer, or mitigation (reduction) [22]. For responding to any unacceptable risk which cannot be avoided or transferred to another party, a proper safeguard should be implemented (risk mitigation).

An information security safeguard (control or countermeasure) is a procedural or technical activity used to reduce the risk to the organization's assets, thereby minimizing any potential loss. Safeguards may involve preventive, detective, or corrective actions [12]. ISO/IEC 7498-2 classifies information security safeguards in the following five categories [6]: *Authentication*, *Access control*, *Data confidentiality*, *Data integrity*, and *Non-repudiation*. At the time a safeguard for a specific risk is chosen, the options should be evaluated based on the cost and amount of risk reduction provided [76], [82], [85], [94]. The selected safeguards then need to be grouped into solution sets which may reduce the risk of several scenarios [12], [42].

After the selected safeguards have been implemented, some risk still remains, and this is called residual risk. The objective of information security risk management is to continuously measure the residual risk and keep it at or below the organization's risk acceptance level [12].

D. Monitoring Risk

Continuous monitoring plays an important role in the field of information security. For almost every information security standard, methodology, or model, there is some kind of monitoring or assessment that should be conducted regularly, and the results need to be carefully documented [34], [40], [62], [72]. In this phase, the effectiveness of the risk management processes can be ensured, as can the alignment of the planned risk responses with the organization's missions, government regulations, policies, standards, and guidelines [34].

IV. A Taxonomy of ISRA Approaches

The challenging part in information security risk assessment (ISRA) process is risk analysis, subsection III.B.1. Therefore, our contribution lies on this part. The proposed taxonomy can aid organizations to have well understanding of risk. In the following, we introduce briefly our taxonomy, and then, the existing risk assessment approaches in relation to the proposed taxonomy are provided in Section V.

As illustrated in Figure 1, information security risk assessment approaches are generally classified in four categories: *Appraisement*, *Perspective*, *Resource Valuation*, and *Risk Measurement*. These categories do not mean to be exclusive, and organizations should attempt to build approaches that do fall into all four.

A. Appraisement (C_1)

Information security risk assessment appraisements can be classified into three categories: *Quantitative*, *Qualitative*, or *Hybrid*.

1) Quantitative: Quantitative appraisement relies on hard numbers, lengthy and time-consuming calculations, probability theory, and statistics to determine the level of an organization's risk exposure [14], [43]. Quantitative risk assessment is based on objective measurements, and the results can be expressed in a management-specific language (i.e. monetary value, percentages, and probabilities) [6]. The inputs and outputs of quantitative risk assessment can be classified in two categories: *monetary* and *non-monetary*. In monetary evaluation, a monetary value is assigned to every asset, vulnerability, threat, and safeguard implementation. In contrast, non-monetary evaluation yields a non-monetary number.

Quantitative appraisement is also known as "expected value analyses" (EV) [24]. In these ap-

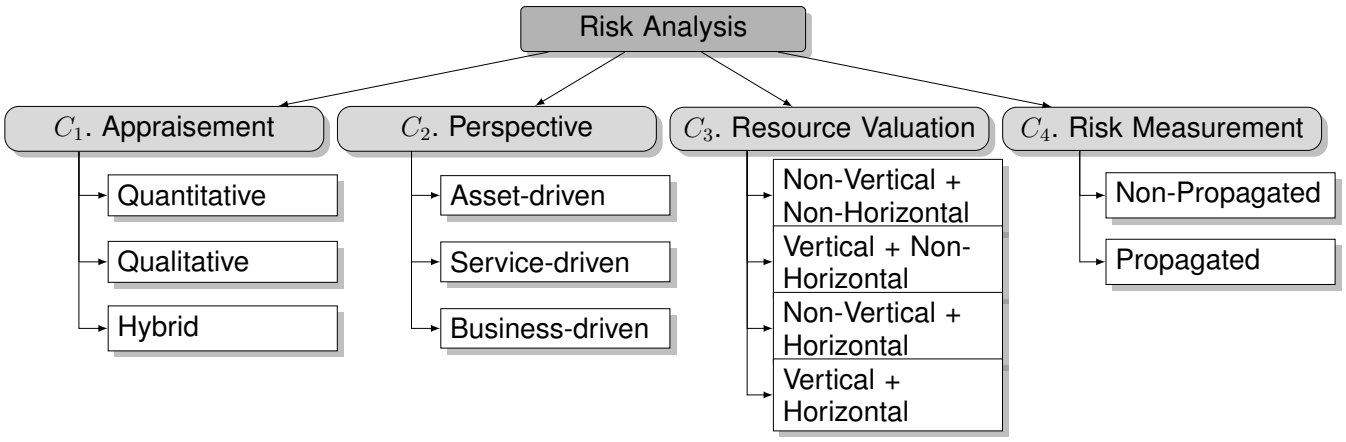

Fig. 1: A taxonomy of Information Security Risk Assessment (ISRA) approaches.

praisements, the impact of each scenario is assessed based on the expected loss to the organization caused by that scenario. The calculated impact, along with the probability of the threat, forms a particular scenario's quantitative risk. The best known EV appraisements are Annualized Loss Expectancy (ALE) and the Livermore Risk Analysis Methodology ($LRAM$) [25], [58].

The major problem with the quantitative appraisements is the lengthy and time-consuming process, which depends to the detailed information. Information such as the value of the assets and the sufficient historical incident data is used to calculate the expected loss and determine the probability. Due to the limited time, money, and human resources available faced by organizations, implementing this approach will not be easy [14], [33].

2) Qualitative: The most common appraisement to information security risk assessment is the qualitative appraisement, and many organizations find it sufficient for their needs [12]. In a qualitative appraisement, classes and relative values are used to show the impact and probability of a particular scenario. Information security risks are assessed using methods and principles with non numerical (qualitative) levels [34]. The input and output of qualitative risk assessment can be classified in two categories: *range variables* and *linguistic variables* for input, and *range variables* and *rank variables* for output. In the range category of variables, which applies to both input and output, the qualitative appraisement rates risks in a qualitative risk matrix, which comprises a vulnerability measure and a threat likelihood measure, each of which is expressed on a scale of three to five levels (e.g. low, medium, and high) [15]. In the linguistic category of variables, expert opinion is used to weight criteria and rate alternatives. The concept of a linguistic variable is very useful for dealing with situations that are not well defined [54]. Some qualitative appraisements (e.g. [69]) are designed to rank and prioritize the risks that an organization typically faces.

The qualitative appraisements are widely used, because there are often not enough accurate historical data to calculate the impact and probability of occurrence of risk scenarios, and also because they are much easier to understand and implement [15]. Also, with these appraisements, the calculations involved are simpler and the valuation of assets, threats, and vulnerabilities is easier [34]. However, they lack of sufficient measurable detail to support cost-effective decision making by management [14]. Moreover, they are based on the knowledge and experience of those involved in the process (assessors and stakeholders), which makes these appraisements more subjective and prone to error and imprecision than their quantitative counterparts [15]. Another problem with the traditional qualitative appraisements is that the range of values assigned to information assets, their vulnerability level, and the threat likelihood is comparatively small, which makes it difficult to prioritize information security risks and compare the associated risk assessment results [34].

3) Hybrid (Semi-quantitative): Because of the strengths and weaknesses of both the quantitative and qualitative appraisements, it is an axiom of information security risk assessment that a combination of the two, a hybrid appraisement, be used [45]. In this way, the organization can benefit from the simplicity and speed of the qualitative appraisements, while taking advantage of the quantitative appraisement for its more critical assets.

B. Perspective (C_2)

There are three perspectives to analyze risks: *Asset-driven*, *Service-driven*, and *Business-driven*. The main focus of this category is to choose a level of the organization's resources (i.e. asset, service, or business process) to identify their corresponding risks. The asset-driven perspective identifies the assets and their associated risks in asset level, whereas the Business-driven identifies risks to the business processes directly. The Service-driven perspective, on the other hand, uses services as input of risk assessment and considers risks to services rather than assets or business processes. In this section, these three risk assessment perspectives are explained in details.

1) Asset-driven: Asset-driven is the most common perspective to risk assessment. In this perspective, assets are identified and evaluated, and then the associated risks are calculated. To achieve a desired level of information security, an ISRA approach must identify the organization's valuable information assets and systematically measure the risks to which they are exposed [23]. In an asset-driven approach, the threats and vulnerabilities to each asset are identified, and the risk scenarios are formed. There are thousands of assets in a medium to large organization, and this number multiplied by the average number of risk scenarios for each information asset gives rise to huge lists of risk scenarios, which need to be analyzed and maintained on a regular basis. This is the main weakness of the asset-driven perspective, and it makes risk assessment a tedious and error-prone task. The main advantage of asset-driven approaches is that they are easier to understand, and because of their widespread usage, the majority of tools available on the market are designed based on this perspective.

2) Service-driven: In service-driven perspective, risks are identified and assessed based on their impact on the services. In this perspective, all of the important services and service packages of the organization are identified first. As opposed to asset-driven approaches, a Service-driven perspective identifies the threats and vulnerabilities for each service and not for individual assets. Since the number of services in an organization is considerably less than the number of assets, a Service-driven approach is easier to manage.

3) Business-driven: The Business-driven security risk assessment approaches are based on business goals and the processes supporting these goals [77]. In this perspective, values are not assigned to assets, but rather to processes that are directly linked to business goals. The business processes of a company are better understood and easier to estimate than information assets. The main focus in Business-driven perspective lies on identifying and analyzing the business processes and their related vulnerabilities and threats. Because of the direct linkage of this perspective to organization's goals and objectives, the risk assessment results could be much easier to explain for the top management and acquire the needed support.

C. Resource Valuation (C_3)

An important stage in risk analysis is to identify the value of resources (i.e. assets, services, business processes). As seen in Figure 2, there is a connection between our selection in category $C2$ (Perspective) and the number of options in category $C3$. For example, if we adopt an Asset-driven perspective and identify the risks on the asset level, consequently, we will need to determine the value of each asset. Likewise, for a Service-driven or Business-driven perspective, the service value or business process value will be needed, respectively. The three types of resources, which we have mentioned before, are not completely isolated from each other and may have horizontal and/or vertical connections (Figure 3). As a result, resource valuation can be obtained from two views: 1) *Vertical View* and 2) *Horizontal View*.

1) Vertical View: The vertical view is a bottom-up view and it considers the resources' contribution degree of a level in the upper level as illustrated in

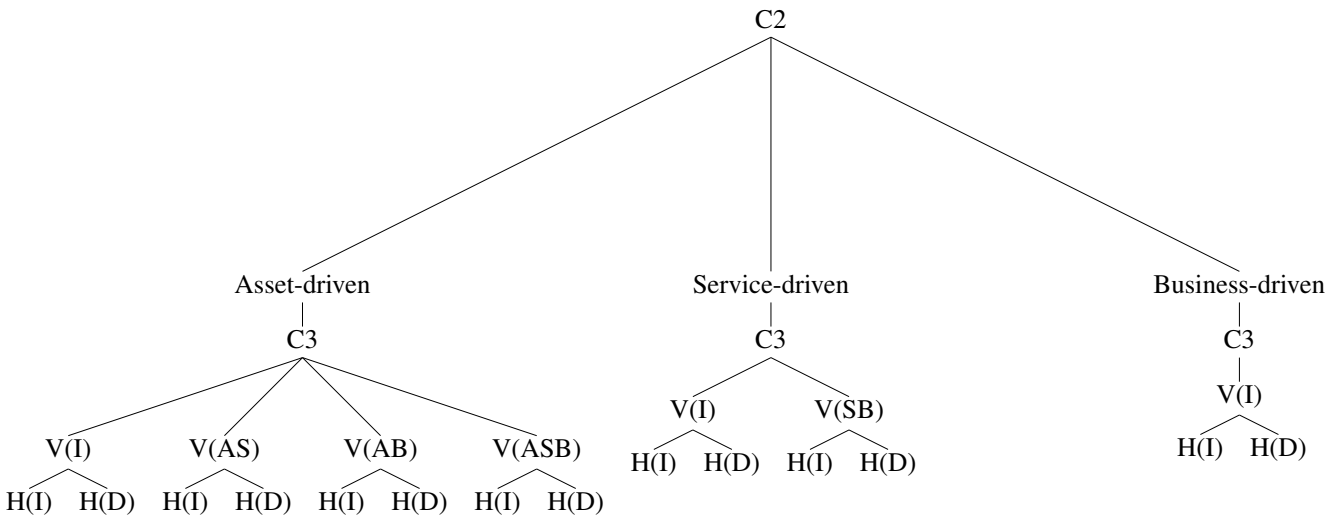

Fig. 2: The relationship between categories C_2 and C_3.

Figure 3. For example, if we decide to determine the asset value, there are four options to choose from: 1) considering the asset itself, without its contribution into the other levels (called, V(I) (Vertical (Independent)), 2) considering the contribution degree of assets in the organization's services (called, V(AS) (Vertical (Asset to Service)), 3) considering the contribution degree of assets in the organization's business processes (called, V(AB)), and 4) considering the contribution degree of assets in the organization's business processes through services (called, V(ASB)).

If we decided to evaluate security risks based on services (Service-driven), there are two options: V(I) and V(SB). Since the business level is the last level in bottom-up view, the vertical view does not make sense in this level.

The result of the resource valuation may differ based on the vertical view. For example, imagine two routers with the same properties in two different departments of a company (Finance and R&D). If we choose the V(I) view, the values of these two routers are the same, while in V(AB) view the one that is more critical to the company's business processes should be assigned a higher severity level [80].

Although vertical view produces realistic estimates of resource value, the adopted view makes it difficult to consider all of those dependencies in determining the resource value.

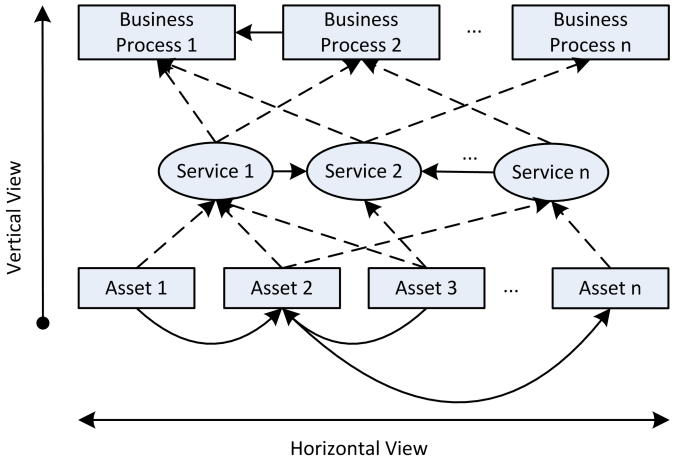

Fig. 3: Resource valuation views: vertical view notes the dependencies between resources of different levels, while the horizontal view refers to the dependencies between resources at the same level.

2) Horizontal View: While vertical view notes the dependencies between resources of different levels, the horizontal view refers the dependencies between resources at the same level. Generally, resource valuation in horizontal view can be classified into two models: *Independent* and *Dependent*. These two horizontal models are presented as H(I) (Horizontal(Independent)) and H(D) (Horizontal(Dependent)) in Figure 2. In the first model which is called independent, the resource evaluation is considered in isolation from the evaluation of other resources at the same level.

Dependent model considers the dependencies between resources in the current level to compute the accurate value of each resource by resource dependency graph. Dependent model refers to this fact that resources are not independent and their values usually depend on others. There are different kinds of dependencies between resources [88], [89], depending on the confidentiality, integrity, or availability property. Jahnke et al. [88] present a complete dependency list between resources:

- *Mandatory*: it requires the functionality of a resource on which it directly depends on.
- *Alternative*: it requires the functionality of one of all the resources on which a resource depends on.
- *Combined*: it simultaneously requires the functionalities of all the resources on which a resource depends on.
- *m-out-of-n*: it needs the functionality of at least *m* among *n* resources.
- *Indirect*: the functionality of a resource is immediately affected when the functionality or direct accessibility of at least one resource it directly or indirectly depends on is limited.

D. Risk Measurement (C_4)

Risk measurement is the final step of risk assessment. We distinguish two types of measurements: *Non-Propagated* and *Propagated*.

1) Non-Propagated: In this model, risk is measured regardless of its impact propagation to other resources. For example, imagine our perspective in the second category is Business-driven. It means we decided to extract risks based on business processes. As a simple example, risk measurement can be evaluated by multiplying three parameters: business process value, vulnerability effect, and threat effect. As seen, risk is measured regardless of its impact propagation from the compromised business process to other dependent business processes.

2) Propagated: The impact of the attack on the compromised resource is usually propagated to other resources [86], [88], [89]. In this model, the resource dependency graph is used to measure the propagated risk. For example, if a node has some vulnerabilities, it might propagate its correlative risk to connected nodes. When a resource is compromised, two kinds of propagation can be distinguished: *Backward* and *Forward*. Backward impact represents the impact propagation on all services that have functional dependency on the compromised resource, directly or indirectly. In contrast, forward impact refers to the impact propagation from the compromised resource to all dependent resources with respect to the permission type between dependent resources.

In a DoS attack type, the backward effect will be on availability, while in the *User to root (U2R)* or *Remote to local (R2L)* attack types, the effect will be on all the CIA parameters. Suppose that the Apache service has a dependency on the MySQL service. If the attacker attempts to run an attack of type U2R on MySQL service, the Apache service will not send correct information to the website.

In the forward impact propagation, if the attacker obtains root permission for a resource, he can forward damage based on the predefined permission between the compromised resource and all dependent resources. If the permission type is full-access, the attacker can affect all the CIA parameters (if the type of attack is U2R or R2L) or only resource availability (if the attack type is DoS). However, if the permission type is read-only, then only availability is affected, no matter what the attack type is.

The main advantage of the propagated risk measurement is that it can predict the potential damage cost which may be done by the attacker in the next step. But the calculation needs the accurate knowledge about the type of attack, the dependency severity between resources in terms of confidentiality, integrity, and availability, and the type of predefined access permission between resources.

V. Classification of Existing Approaches

An overview of the research and development of information security risk assessment approaches in the last decade is given in Table I. In this section, we will discuss some of them briefly in relation to the proposed taxonomy.

A. Quantitative vs. Qualitative vs. Hybrid

1) Quantitative: Karabacak and Sogukpinar [71] propose a survey-based quantitative appraisement to analyze security risks by taking current needs into consideration. The survey is composed of questions

which are asked of managers, directors, technical personnel, and computer users. Two separate and independent survey processes are conducted, one for each of the two attributes of risk: probability and consequences. The proposed model does not make Single Loss Expectancy (SLE) or ALE calculations during the risk calculation. The risk factor in the appraisement is a numerical value between 1 and 25, and these values correspond to a qualitative appraisal of high, medium, or low. This model uses addition, multiplication, and division operations to calculate risk. This simple model may lead to the effective participation of managers and staff in the risk assessment process.

2) Qualitative: Guan et al. [64] assess information security risks according to the likelihood of occurrence of damage and its potential impact. They categorize risk factors according to the ISO 17799 standard, which is similar to determining the weights of the risk factors in pairwise comparisons in the Analytic Hierarchy Process (AHP) appraisement, in which the likelihood of occurrence of damage to an asset or the weight of each risk factor is determined based on expert opinion. At the same time, the vulnerability of each information asset to each risk factor is considered equal to its impact severity, which takes its relative value from experts through linguistic variables.

3) Hybrid: Deng et al. [57] present a hybrid appraisement which can accommodate imprecise information and uncertain data, along with expert knowledge. They propose combining two elements of risk for each component: likelihood of system failure and the consequences of such a failure (severity of loss). These elements can be described linguistically by domain experts based on fuzzy set theory and the Dempster-Shafer mathematical theory of evidence (DST), which is used to combine the risks of individual components to determine the overall system risk. The authors demonstrate their proposed risk analysis approach through a numerical example. Performing risk analysis on a large organization can be challenging, owing to a lack of data and insufficient understanding of the mechanisms of failure. A ”semi-quantitative” approach, such as the Deng et al. method described above, can be an effective way to handle this task, and there is broad agreement that this is an appropriate approach under these circumstances, even though the definition of risk varies considerably across disciplines.

B. Asset-driven vs. Service-driven vs. Business-driven

1) Asset-driven: Shameli-Sendi et al. [26] propose the fuzzy expert model for risk assessment in asset level. This model consists of three steps. The goal in the first step is to identify the assets of an IT system and the potential threats associated with it. The golden security triangle (CIA) is used to evaluate assets and calculate threat effects. In the second step, a list of asset vulnerabilities is generated. Then, asset values, vulnerability effects, and threat impacts are calculated. The goal in the final step is to assign a numerical value to the risks.

2) Service-driven: Danfeng et al. [81] present a service-based risk quantitative calculation method (SRQC). The calculation model centers on the services of Next Generation Networks (NGN) and considers the relationship of services. The proposed model reflects the risk degree of the various services and the potential losses situation by the risks in the service layer of NGN. The risk calculation model is based on four layers: network layer, service layer, host layer, and risk elements layer. Risk calculation of network consists of the risk calculation of all network services. The risk calculation of each service is computed with respect to the host which provides that service. And the risk calculation of each host is based on the number of assets and their corresponding vulnerabilities and threats.

3) Business-driven: Khanmohammadi and Houmb [77] propose a security risk assessment approach based on business goals and the processes supporting these goals. In this model, values are not assigned to assets, but rather to processes that are directly linked to business goals. They believe that the business processes of a company are better understood and easier to estimate than information assets. This approach comprises two phases. In the first phase, processes are analyzed and their vulnerabilities identified. The second phase concentrates on assessing the risks posed to each process, the value of which is a reflection of the company’s business goals. The degree of exposure to vulnerabilities is calculated based on the answers to some specific questions. Threat

frequency is determined based on the history of the threats that have arisen in the organization, and is a number in the [0,1] range. To calculate the risk level of process, the process value is multiplied by the sum of the risk levels of all the vulnerabilities of the process, which has been obtained by multiplying the degree of exposure to a vulnerability, the control effects already in place to protect against exploitation of the vulnerability, and the threat level posed by the vulnerability.

C. Horizontal (Independent vs. Dependent) and Vertical (Independent vs. Dependent)

1) Horizontal (Dependent): Letchford and Vorobeychik [68] propose a security model for interdependent assets using Stackelberg games to incorporate the costs and benefits of arbitrary security configurations on individual assets. These are games involving two players: *defender* and *attacker*. The defender is responsible for protecting a set of targets using a fixed set of limited defense resources, while the attacker attacks a target that maximizes his expected utility.

Sawilla and Ou [69] propose their AssetRank technique, which addressees the semantics of the vertices and arcs of dependency attack graphs. This technique is a generalization of Google's PageRank algorithm, which ranks Web pages in Web graphs. AssetRank supports three types of vertex in a dependency attack graph: AND, OR, and SINK. An OR vertex can be satisfied by any of its out-neighbors, an AND vertex depends on all its out-neighbors, and SINK vertices represent the ground facts, which include the existence of vulnerable software, network routes, and the services running on each machine. With this approach, it is possible to consider various types of attackers. To model attacker preferences, every vertex is assigned a success likelihood, which has a different meaning for each type of vertex. Each vulnerability vertex is assigned a value: Unproven (1%), Proof-Of-Concept (40%), Functional (80%), and High (99%), to indicate the probability that an attacker will successfully exploit that vulnerability.

Danfeng et al. [81] present a service dependency model to calculate the services value. The service value is computed by "*service basic value*" and "*service addition value*". To calculate service basic value, three main parameters are considered: *the service type*, *the number of customer*, and *the service profitability*. The service addition value is calculated by considering the dependent services to this service.

2) Vertical (Dependent): Eom et al. [80] propose a model to assess risks with respect to the contribution degree of assets in the organization's business. The proposed model considers different factors like the department utilization, business contribution, and user position to identify the asset value.

Su et al. [79] present a model to map assets to business visions. Then the business vision is used to select the valuable assets. Assets are classified into two categories: *Information* and *Technical assets*. The former represents the data and information, and the latter represents those assets that support the storage and transmission.

3) Horizontal (Dependent) and Vertical (Dependent): Suh and Han [92] propose a vertical and horizontal model for asset valuation. The value of asset is calculated based on the relationship with business model and asset dependency graph in asset level. In asset dependency graph, the nodes of the graph are assets, and the edges are functional requirements with dependency weights. The differences of this model compared to the traditional risk analysis are introducing of an organization investigation stage and the consideration to operational continuity. The proposed model regards the business function as the most important one to be managed. They propose five steps to understand the aim and business activities of an organization.

Loloei et al. [87] present a model for asset valuation regarding assets' dependencies and assets' contribution in business goals. In this work, the dependency in the horizontal level is defined in terms of availability. They believe that the available dependency is not essentially complete. However, an asset may depend to some assets partially, and a dependency percent is defined for any dependency. To model the vertical dependency, a meta-model [90], [91] is used that consists of three layers: *Business*, *Application*, and *Technical* layers. Business Layer includes business artifacts like organizational units, roles, business processes, and information objects. Application layer consists of Information system and how they support business processes. In the technical layer, physical hardware, supporting soft-

ware for components, and communication systems are modeled.

Schmidt and Albayrak [95] present a model to obtain the assets' value from vertical and horizontal views. In the vertical view, the business process values are mapped to IT hardware components in a hierarchical fashion through services. In horizontal view, the relationship between resources is modeled by means of a dependency weighted directed graph. Then this model is combined to IT system vulnerability and threat analysis to derive risk scores. To compute the cost-optimal risk mitigation strategies, discrete-time algorithm has been used.

D. Non-Propagated vs. Propagated

1) Non-Propagated: Sun et al. [24] present a risk assessment model based on the Dempster-Shafer Theory of Belief Functions to model the uncertainties involved in the assessment of the presence or absence of threats and the presence or absence of control measures. The proposed model facilitates the assessment of risk by decomposing the overall information security risk into its sub components and assessing the risks associated with each of them by individually assessing the impact of the threats and controls to specific sub components of the overall risk. With this model, an attempt is made to attune two types of cost in dollar terms. One is the cost for implementing the countermeasures, and the other is the value of the potential loss of the asset owing to the residual risk of threat occurrence, even when countermeasures are in place.

2) Propagated: Alpcan et al. [67] present a quantitative framework for security risk analysis in organizations in which they leverage methods applied to document and image retrieval and the adjusted Page-Rank procedure used by the Google search engine. In the first step, the framework captures risk dependencies within and across business units, security threats/vulnerabilities, and individuals using a graph theory approach. Then the model captures the dynamic evolution of risk as a result of challenging interactions, in contrast to static models, which focus on isolated one-time risks. Finally, using the Risk-Rank family of algorithms, they rank and prioritize the risks in an organization.

Mahmoud et al. [86] propose a quantitative risk assessment approach based on risk propagation and network node correlation. The stages of calculation are as follows: 1) scanning and identifying vulnerable nodes, 2) computing individual risk for each identified, 3) calculating the propagated risk for nodes correlated with vulnerable nodes, 4) computing the total risk for each node in the network, and 5) computing the whole network risk level. To calculate the propagated risk, they consider the asset dependency graph. In the proposed model, the propagation likelihood depends on the likelihood of vulnerability on the issuing node and the likelihood of correlation between the two nodes.

Jahnke et al. [88] present a graph-based approach for modeling the effects of attacks against resources and the effects of the response measures taken in reaction to those attacks. The proposed approach uses directed graphs showing dependencies between resources and derives quantitative differences between system states from these graphs. If we assume that G and $\acute{G}$ are the graphs we obtain before and after the reaction, respectively, then calculation of the response's positive effect is the difference between the availability plotted in the two graphs: $A(\acute{G}) - A(G)$. These authors focus on the availability impacts.

Kheir et al. [89] propose a dependency graph to evaluate the confidentiality and integrity impacts, as well as the availability impact. The confidentiality and integrity criteria are not considered in [88]. In [89], the impact propagation process proposed by Jahnke et al. is extended to include these impacts. Now, each service in the dependency graph is described with a 3D CIA vector. In the proposed model, dependencies are classified as structural or functional dependencies.

VI. Discussion

Although many information security risk assessment approaches have been proposed in the last decade, many organizations find it challenging to address their specific needs with the most appropriate methods [70]. In this paper, we proposed a taxonomy for information security risk assessment approaches that is generally classified in four categories: *Appraisement*, *Perspective*, *Resource Valuation*, and *Risk Measurement*. The most important advantages and disadvantages of these categories are presented in Table II.

TABLE I: Summary of existing information security risk assessment approaches

Title	Perspective	Technique used	Appraisement	Input/Output	Resource Valuation	Risk Measurement	Risk Phases
Professional Organizations							
CRAMM [47]	AD[a]	Multiplication Operation	QL[b]	-	V(I)[c]+H(I)[d]	NP[e]	1. RA[f] 2. RE[g] 3. RR[h]
CORAS [48]	AD	Multiplication Operation	QL	-	V(I)+H(I)	NP	1. RA 2. RE 3. RR
OCTAVE [49]	AD	Multiplication Operation	QL	-	V(I)+H(I)	NP	1. RA 2. RE 3. RR
Magerit V2 [i][50]	AD	Multiplication Operation	QN[j] / QL	-	V(I)+H(I)	NP	1. RA 2. RE 3. RR
Microsoft [51]	AD	Multiplication Operation	HB[k]	-	V(I)+H(I)	NP	1. RA 2. RE 3. RR
Mehari [52]	AD	Multiplication Operation	HB	-	V(I)+H(I)	NP	1. RA 2. RE 3. RR
OCTAVE Allegro [53]	AD	Multiplication Operation	HB	-	V(I)+H(I)	NP	1. RA 2. RE 3. RR
ISO/IEC 27005 [72]	AD	Multiplication Operation	HB	-	V(I)+H(I)	NP	1. RA 2. RE 3. RR
NIST 800-30rev1 [34]	AD	Multiplication Operation	HB	-	V(I)+H(I)	NP	1. RA 2. RE 3. RR
Research Projects							
Guan et al. [64]	AD	Multi-Criteria Decision-Making	QL	Linguistic variables/Range	V(I)+H(I)	NP	1. RA 2. RE 3. RR
Karabacak and Sogukpinar [71]	AD	Mathematical Operations	QN	Non-Monetary/Non-Monetary	V(I)+H(I)	NP	1. RA 2. RE
Sun et al. [24]	AD	Dempster-Shafer Theory	QN	Monetary/Monetary	V(I)+H(I)	NP	1. RA 2. RE 3. RR
Kondakci [65]	AD	Labeling	QN	Non-Monetary/Non-Monetary	V(I)+H(I)	NP	1. RA 2. RE
Shameli-Sendi et al. [26]	AD	Fuzzy	QL	Range/Rank	V(I)+H(I)	NP	1. RA 2. RE
Khanmohammadi and Houmb [77]	BD[l]	Multiplication Operation	QN	Non-Monetary/Non-Monetary	V(I)+H(I)	NP	1. RA 2. RE
Deng et al. [57]	AD	Dempster-Shafer and Fuzzy Set Theory	HB	Non-Monetary/Non-Monetary	V(I)+H(I)	NP	1. RA 2. RE
Lo and Chen [56]	AD	DEMATEL, ANP, FLQ-MEOWA	HB	Non-Monetary/Non-Monetary	V(I)+H(I)	NP	1. RA 2. RE 3. RR
Su et al. [79]	AD	N/A	QL	N/A	V(AB)[q]+H(I)	NP	1. RA 2. RE
Eom et al. [80]	AD	Mathematical Operations	QL	Range/Non-Monetary	V(AB)+H(I)	NP	1. RA 2. RE
Danfeng et al. [81]	SD[n]	Mathematical Operations	QN	Non-Monetary/Non-Monetary	V(I)+H(D)[o]	NP	1. RA 2. RE
Mahmoud et al. [86]	AD	Mathematical Operations	QN	Non-Monetary/Non-Monetary	V(I)+H(I)	P[p]	1. RA 2. RE
Loloei et al. [87]	AD	Mathematical Operations	QN	Non-Monetary/Non-Monetary	V(AB)+H(D)	NP	1. RA
Jahnke et al. [88]	SD	Mathematical Operations	QN	Non-Monetary/Non-Monetary	V(I)+H(I)	P	1. RA 2. RE 3. RR
Kheir et al. [89]	SD	Mathematical Operations	QN	Non-Monetary/Non-Monetary	V(I)+H(I)	P	1. RA 2. RE 3. RR
Letchford and Vorobeychik [68]	AD	Game Theory	QL	Non-Monetary/Non-Monetary	V(I)+H(D)	NP	1. RA 2. RE
Suh and Han [92]	AD	Mathematical Operations	QN	Monetary/Monetary	V(AB)+H(D)	NP	1. RA 2. RE
Alpcan and Bambos [67]	AD	Graph-theoretic	QN	Non-Monetary/Non-Monetary	V(I)+H(I)	P	1. RA 2. RE
Sawilla and Ou [69]	AD	Attack Graph	QL	Rank/Rank	V(I)+H(D)	NP	1. RA 2. RE
Samantra et al. [93]	AD	Fuzzy set theory	QL	Linguistic variables/Range	V(I)+H(I)	NP	1. RA 2. RE 3. RR
Schmidt and Albayrak [95]	AD	Mathematical Operations	QN	Monetary/Monetary	V(ASB)[q]+H(D)	P	1. RA 2. RE 3. RR
Houmb et al. [75]	AD	Bayesian Belief Network	HB	Non-Monetary/Non-Monetary	V(I)+H(I)	NP	1. RA 2. RE 3. RR

[a] Asset-driven [b] Qualitative [c] Vertical view is independent [d] Horizontal view is independent [e] Non-Propagated [f] Risk Analysis [g] Risk Evaluation
[h] Responding to Risk [i] It can be applied both quantitatively and qualitatively [j] Quantitative [k] Hybrid [l] Business-driven [m] Vertical view is dependent (asset to business)
[n] Service-driven [o] Horizontal view is dependent [p] Propagated [q] Vertical view is dependent (asset to service to business)

As discussed, information security risk assessment appraisements can be quantitative, qualitative, or hybrid. Organizations base their choice on their culture and their attitude toward risk [61]. As we have seen, the existing qualitative and quantitative information security risk assessment approaches are subject to a number of weaknesses, problems, and constraints [24], [63]. In quantitative risk assessment, the goal is to assign objective numerical values to information assets, risks, safeguards, and impacts using statistical tools [51], [56], [60]. A great deal of work is required to precisely determine the monetary value of information assets, the frequency of threats, and the cost of controls [6], [51], [56], [66]. As mentioned, Annualized Loss Expectancy (ALE) is one of the most influencing quantitative approaches. There is no adequate information in ALE on how to calculate the Exposure Factor (*EF*). The majority of quantitative risk assessment approaches do not provide a means to calculate *EF* with a standard method, and leave this task to the user [25]. Calculating the Annualized Rate of Occurrence (*ARO*) is equivalent to the probability of a threat arising to an information asset, and is yet another ambiguity in ALE. The *ARO* is usually calculated based on the history of the incidents that have occurred and the advice of information security experts [4]. These probabilities are not easy to estimate, and existing methods only provide users with some general suggestions and examples, leaving them to take care of the large number of interrelated relevant factors [24]. Moreover, the quantitative appraisement, which presents results in monetary terms only, may be difficult for non-technical individuals to interpret [51], [56].

In contrast, qualitative risk management appraise-

TABLE II: Summary of advantages and disadvantages of each element of the proposed taxonomy

	Advantages	Disadvantages
Appraisement		
Quantitative	• Risks levels may be identified in monetary terms • Results can be expressed in management-specific language • Great effort is put into resource value definition and risk mitigation • Cost-benefit assessment effort is possible	• Estimating the damage probability of each resource is imprecise • The numerical/monetary results may be difficult for non-technical people to interpret • Calculation can be challenging, expensive, and time consuming
Qualitative	• It is not necessary to quantify threat likelihood • Prioritizes the risks and identifies areas for immediate action and improvement • Save time, effort, and expense • Easier to involve people who are not experts on security or computers	• Does not provide monetary values and probabilities • Making a cost-benefit analysis of recommended controls is more difficult • Very subjective and prone to errors and imprecision
Hybrid	• It has the flexibility to change quantitative inputs to qualitative outputs and vice versa	
Perspective		
Asset-driven	• The majority of tools available on the market are designed based on this perspective • It needs less expertise and is easy to understand	• Makes the calculation error-prone for the large number of resources in a medium to large organization • It makes the risk reduction inefficient
Service-driven	• Services are easier to evaluate • Services are better understood and easier to identify and grasp than assets • Save time and effort in large organizations	• May be too challenging for small organizations • It is more suitable for those organizations, which have a service-based approach in delivering their business processes
Business-driven	• Those risks that have high impact in organization can be seen well in output of risk assessment • Business processes can be better evaluated even based on their financial impact • Business processes are better understood and easier to explain for the top management and acquire the needed support • It leads to an efficient risk reduction	• May be too challenging for small organizations • It needs more insight into the business and its processes
Resource Valuation		
Horizontal and Vertical Views (Independent)	• Calculation is simple	• Imprecise • The value of the resources are close to each other and makes it hard to detect important resources • The value of resources are not based on their impact on other resources
Horizontal and Vertical Views (Dependent)	• It produces more realistic estimates of resource value • It facilitates to separate critical and non-critical resources	• It needs to keep track of dependencies between resources • It needs to extract the different kind of dependencies between resources • It needs a good understanding about which resources are dependent to each other
Risk Measurement		
Non-Propagated	• It makes the risk measurement easy for the large number of risks and resources	• Imprecise • It may lead to select inappropriate security safeguards • Does not have the ability to estimate the potential damage cost in the future
Propagated	• Risks are calculated more accurately • It indicates exactly what part of the network will be affected by attack • It can predict the potential damage cost which may be done by the attacker in the next step	• It needs the accurate knowledge about the type of attack, the dependency severity between resources in terms of confidentiality, integrity, and availability, and the type of predefined access permission between resources • A thorough change management is needed to update dependencies • Makes hard to utilize for a big resource dependency graph

ments are based on judgment (which is subjective in nature), and experts assign relative values to the information assets, risks, safeguards, and impacts [43], [51], [56], [73]. The problem with the qualitative appraisements is the lack of sufficient measurable detail, which reduces its value to decision makers [14], [63], as the results of the qualitative appraisement are hugely dependent on the security experts who conduct the risk analysis [71]. In an effort to get rid of the weaknesses of the these two appraisements, some models combine their best features into a unique, hybrid appraisement. However, an appraisement that seems ideal for one situation, budget, or industry may not be suitable for others, and there is no "one-size-fits-all" appraisement [12], [44]. To secure valuable information, organizations need to invest large sums in developing information security countermeasures. Management needs to be convinced that it is reasonable to make these investments rather than spend the funds elsewhere [46]. The decision as to which appraisement, quantitative, qualitative, or hybrid, is more appropriate, depends on many factors [59]: 1) the needs of the decision-makers, 2) the credibility of the available appraisements, 3) budget, 4) availability of the statistical data, and 5) availability of the financial data.

There are three perspectives to analyze risks: *Asset-driven*, *Service-driven*, and *Business-driven*. As seen in Table I, most of the risk assessment models are Asset-driven. The Asset-driven risk assessment model suffers from some limitations. First, the total number of an organization's assets is usually high, and this reduces the accuracy of their valuation. Second, determining the monetary value of assets, threat frequency, and cost of controls needs a large amount of work to be precise [6], [51], [56], [66]. We need to take the following information into account to evaluate an information asset [15]: a general description of the asset, its function and features, its classification, its criticality to the organization, applicable regulations, and the user community. It is clear that calculating the value of an information asset (e.g. a switch, a firewall, or a database) with all these criteria in mind would be quite difficult and time consuming, and not easy to do accurately. Third, the output of the risks is extremely close to each other and makes it hard to detect significant risks. Finally, the risk reduction phase of this model is inefficient due to the proximity of risks. In contrast, Service-driven and Business-driven models try to address all Asset-driven model weaknesses. As seen in Table I, some studies believe that information security risk analysis should be more service or business oriented [77], [81]. In these two perspectives, the focus of extracting resources and risks is on services or business processes rather than assets. The reason for this is that a service or business process is directly involved in business revenue and then is better understood in risk assessment.

Resource valuation, the third category, can be performed independently or dependently. The dependency model can be considered in vertical view or horizontal view. As shown in Table I, most of the proposed models treat resources as independent, obviating the need to consider resource interdependency in neither vertical nor horizontal view. Since this model is simple, calculations can be simplified but it suffers from the fact that the resource value may be inaccurate. In contrast, the dependent model considers the dependencies between resources to compute the accurate value of each resource by a resource dependency graph. There are some works that consider resource dependency in the valuation process: Horizontal View [68], [69], [81], Vertical View [79], [80], and both [87], [92], [95]. The great advantage of this model is that it produces realistic estimates of resource value. The main disadvantage of this model is that all dependencies between resources should be extracted and it would be time-consuming for a company with large number of assets.

The fourth category, Risk Measurement, is classified into two sub-categories: *Non-Propagated* and *Propagated*. As seen in Table I, the most common approaches used for risk assessment lie on non-propagated sub-category. In fact, risk impact is calculated regardless of possible security dependency relations between nodes and risk propagation concepts. This model is easy to deploy and flexible enough for those companies which are not looking for accurate ISRA model especially with a large number of risks and resources. The main disadvantage of this model is that the risk impact value does not cover the potential damage. There are a few works which investigate risk propagation

between dependent resources [67], [86], [88], [89]. The propagation model indicates exactly what part of the network will be affected by attack. Thus, this model leads to select appropriate security safeguards.

Hybrid Appraisement, Business-driven perspective, Resource Valuation through dependency graph in vertical and horizontal views, and risk measurement using propagation concept are the four main findings of this survey paper. We believe that the perfect coordination between them leads to an efficient framework for ISRA that is able to assess and mitigate risk accurately.

VII. Conclusion

Many organizations use information systems and network frameworks on a large scale, and so the dependency on IT is increasing daily. Security is one of the most important issues for the stability and development of these systems. Therefore, most of the organizations invest in this area and are establishing Information Security Management Systems (ISMS). Information Security Risk Assessment (ISRA) is an essential element of ISMS process. Organizations need ISRA to identify security risks and to help them choose the best safeguards to reduce them. Because there are so many types of risk assessment approaches available, organizations are still in doubt on how to choose the ideal method for their specific needs.

The old taxonomy of risk assessment classifies ISRA approaches based on three criteria: quantitative, qualitative, and hybrid. The primary focus of this old taxonomy is on the type of input and output of risk calculation. There are some points that are hidden in the body of risk evaluation process and should be taken into account. The current tools or methodologies fail to answer fundamental questions in risk assessment: 1) How do we separate critical and non-critical resources? 2) Is there a mechanism to consider the contribution degree of resources in the company's business goal? 3) How do we model the dependency severity between resources? 4) How do we calculate the likelihood of a threat? and 5) How do we model the real impact propagation from the compromised resource to other resources?

In the risk assessment, we need to recognize the important and critical resources, and the risk management should be done for them properly. On the other hand, we require an accurate picture of attack damage propagation from the compromised resource. We need to know the result of attack propagation in backward and forward directions in the resource dependency graph from the compromised resource. For example, how much is the impact propagation on all resources that have functional dependency to the compromised resource, directly or indirectly? Or how much is the impact propagation from the compromised resource to all dependent resources with respect to the permission type between dependent resources?

Due to the large number of methodologies and frameworks available for evaluating risk, organizations have not met their demands. Lack of attention to discussed questions in the risk assessment process causes many challenges: 1) the number of non-critical resources rises, 2) the effect of the threat could not be accurately calculated, 3) the output of the risks is extremely close to each other and makes it hard to detect significant risks, and 4) the evaluation of the risk is too imprecise, and this leads to a lack of proper risk management in the next step.

Taxonomy presented in this paper is a step toward achieving high-quality ISRA. The old taxonomy is one element of our proposed taxonomy. In the current study, we discovered other important elements that should be considered in risk assessment. Our objective is to provide organizations with an overview of the various techniques used to evaluate risks. This can help them conduct risk assessment successfully.

Acknowledgments

This work is partly funded by Natural Sciences and Engineering Research Council of Canada Research Chair on Sustainable Smart Eco-Cloud, NSERC-950-229052 and by the NSERCCRDPJ 424371-11: ECOLOTIC Sustainable and Green Telco-Cloud.

References

[1] S. C. Misra, V. Kumar, and U. Kumar, "A strategic modeling technique for information security risk assessment," Information Management & Computer Security, vol. 15, no. 1, pp. 64-77, 2007.

[2] International Organization for Standardization, ISO/IEC 27002:2013 Information technology Security techniques Code of practice for information security management, Geneva: ISO, 2013.

[3] A. Borek, A. K. Parlikad, J. Webb, and P. Woodall, "Total Information Risk Management: Maximizing the Value of Data and Information Assets," Massachusetts: Elsevier, 2013.

[4] S. Harris, CISSP All-in-One Exam Guide, 5th ed., New York: McGraw Hill, 2010.

[5] A. Calder and S. Watkins, IT Governanace: A Manager's Guide to Data Security and ISO 27001/ISO 27002, 4th ed., London: Kogan Page Ltd., 2008.

[6] F. Farahmand, S. B. Navathe, G. P. Sharp, and P. H. Enslow, "A Management Perspective on Risk of Security Threats to Information Systems," Information Technology and Management, vol. 6, no. 2-3, pp. 203-225, 2005.

[7] Ponemon Institute LLC, "Cost of Data Breach Study: United Kingdom," 2012. [Online]. Available: http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-uk.en-us.pdf. [Accessed March 2014].

[8] S. Wilcox and B. Brown, "Risk Assessment, Risk Management, and the HIPAA Security Rule: A Matter of Life and Death?," Journal of Health Care Compliance, vol. 6, no. 4, pp. 43-45, 2004.

[9] B. Nikoli and L. Rui-Dimitrijevi, "Risk assessment of information technology systems," Informing Science and Information Technology, vol. 6, pp. 595-615, 2009.

[10] J. Smith, "Getting the Right Balance: Information Security and Information Access," Legal Information Management, vol. 10, no. 1, 2010.

[11] P. Foreman, "Vulnerability Management," Boca Raton: Auerbach Publications, 2010.

[12] D. J. Landoll, "The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments," 2nd ed., Boca Raton: Auerbach Publications, 2006.

[13] S. Strecker, D. Heise, and U. Frank, "RiskM: A multi-perspective modeling method for IT risk assessment," Information Systems Frontiers, vol. 13, no. 4, pp. 595-611, 2011.

[14] E. Hulitt and R. B. Vaughn, "Information system security compliance to FISMA standard: a quantitative measure," Telecommunication Systems, vol. 45, no. 2-3, pp. 139-152, 2010.

[15] E. Wheeler, "Security Risk Management: Building an Information Security Risk Management Program from the Ground Up," Waltham: Syngress, 2011.

[16] D.-L. Huang, P.-L. P. Rau, and G. Salvendy, "Perception of information security," Behaviour & Information Technology, vol. 29, no. 3, pp. 221-232, 2010.

[17] C. Young, Metrics and Methods for Security Risk Management, Burlington: Syngress, 2009.

[18] D. Apgar, "Measure Your Risk IQ: What you don't know can hurt you. Risk intelligence helps prioritize information-security projects," Optimize, vol. 5, no. 10, pp. 32-38, 2006.

[19] Z. Jourdan, K. R. Rainer Jr, and T. E. Marsh, "An Investigation Of Organizational Information Security Risk Analysis," Journal of Service Science (JSS), vol. 3, no. 2, pp. 33-42, 2010.

[20] G. Sadowsky, J. X. Dempsey, and A. Greenberg, Information Technology Security Handbook, Washington: World Bank, 2003.

[21] A. Shameli-Sendi, M. Jabbarifar, M. Dagenais, and M. Shajari, "System Health Monitoring Using a Novel Method: Security Unified Process," Journal of Computer Networks and Communications, 2012.

[22] A. Jones, "A framework for the management of information security risks," BT technology journal, vol. 25, no. 1, pp. 30-36, 2007.

[23] P. Shedden, R. Scheepers, W. Smith, and A. Atif, "Incorporating a knowledge perspective into security risk assessments: Very Informal Newsletter on Library Automation," VINE, vol. 41, no. 2, pp. 152-166, 2011.

[24] L. Sun, R. P. Srivastava, and T. J. Mock, "An information systems security risk assessment model under the Dempster-Shafer theory of belief functions," Journal of Management Information Systems, vol. 22, no. 4, pp. 109-142, 2006.

[25] A. Asosheh, B. Dehmoubed, and A. Khani, "A new quantitative approach for information security risk assessment," in 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2009, 2009.

[26] A. Shameli-Sendi, M. Jabbarifar, M. Shajari, and M. Dagenais, "FEMRA: Fuzzy Expert Model for Risk Assessment," in the Fifth International Conference on Internet Monitoring and Protection (ICIMP), pp. 48-53, 2010.

[27] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security Ontologies: Improving Quantitative Risk Analysis," in The 40th Hawaii International Conference on System Sciences, Hawaii, 2007.

[28] Kaspersky Lab, "Global IT Security Risks: 2012," 2013. [Online]. Available: http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf. [Accessed March 2014].

[29] Verizon, "2012 Data Breach Investigations Report," 2012. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf. [Accessed March 2014].

[30] International Organization for Standardization, ISO/IEC 27000:2012 Information technology Security techniques Information security management systems Overview and vocabulary, Geneva: ISO, 2012.

[31] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," Security & Privacy, IEEE, vol. 4, no.6, pp. 85-89, 2006.

[32] G. A. Holton, "Defining risk," Financial Analysts Journal, pp. 19-25, 2004.

[33] F. Farahmand, S. B. Navathe, P. H. Enslow, and G. P. Sharp, "Managing vulnerabilities of information systems to security incidents," in The 5th international conference on Electronic commerce, 2003.

[34] NIST, "NIST SP - 800-30rev1," 2012. [Online]. Available: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091. [Accessed March 2014].

[35] A. Stango, N. R. Prasad, and D. Kyriazanos, "A threat analysis methodology for security evaluation and enhancement planning," in Third International Conference on Emerging Security Information, Systems and Technologies SECURWARE, 2009.

[36] T. Iijima and J. Curtis, "Need to justify IT security? Measure your risk!," The Journal of Corporate Accounting & Finance, vol. 15, no. 5, pp. 47-51, 2004.

[37] R. Ross, "Managing Enterprise Risk in Today's World of Sophisticated Threats: a Framework for Developing Broad-Based, Cost-Effective Information Security Programs," EDPAC: The EDP Audit, Control, and Security Newsletter, vol. 35, no. 2, pp. 1-10, 2007.

[38] Z. I. Saleh, H. Refai, and A. Mashhour, "Proposed Framework for Security Risk Assessment," Journal of Information Security, vol. 2, no. 2, pp. 85-90, 2011.

[39] S. Liu, R. Kuhn, and H. Rossman, "Understanding insecure IT: practical risk assessment," IT professional, vol. 11, no. 3, pp. 57-59, 2009.

[40] International Organization for Standardization, ISO/IEC 27001:2013 Information technology Security techniques Information security management systems Requirements, Geneva: ISO, 2013.

[41] NVD, "National Vulnerabilities Database," 2013. [Online]. Available: http://nvd.nist.gov/cpe.cfm. [Accessed March 2014].

[42] A. C. Pinto, A. Aurora, and D. E. Hall, "Challenges to Sustainable Risk Management: Case Example in Information Network Security: EMJ," Engineering Management Journal, vol. 18, no. 1, pp. 17-23, 2006.

[43] S. Lichtenstein, "Factors in the selection of a risk assessment method," Information Management & Computer Security , vol. 4, no. 4, pp. 20-25, 1996.

[44] H. Cavusoglu, B. Mishra, and S. Raghunatan, "A model for evaluating IT security investments," Communications of the ACM, vol. 47, no. 7, pp. 87-92, 2004.

[45] G. Guglielmo, "Analyzing and Prioritizing Risk in IT Security: Methods for Gathering Information in a Dynamic Environment," Commercial Law Bulletin, vol. 19, no. 4, pp. 20-23, 2004.

[46] L. A. Gordon and M. P. Loeb, "Return on information security investments: Myths vs. realities," Strategic Finance, vol. 84, no. 5, pp. 26-31, 2002.

[47] CRAMM user guide, Risk Analysis and Management Method, United Kingdom Central Computer and Telecommunication Agency (CCTA), UK, 2001.

[48] F. den Braber, I. Hogganvik, M. S. Lund, K. Stlen, and F. Vraalsen, "Model-based security analysis in seven stepsa guided tour to the CORAS method," BT Technology Journal, vol. 25, no. 1, pp. 101-117, 2007.

[49] OCTAVE, Managing Information Security Risk, Carnegie Mellon, USA, 2005.

[50] Magerit, Methodology for Information Systems Risk Analysis and Management: Book1The Method, Ministerio de Administracones Publicas, Madrid, 2006.

[51] The Security Risk Management Guide, Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence, 2006.

[52] Mehari, Overview, Club de la Securite de IInformation Francais (CLUSIF), 2007.

[53] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process (No. CMU/SEI-2007-TR-012)," CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2007.

[54] A. Shameli-Sendi and M. Dagenais, "ARITO: Cyber-attack response system using accurate risk impact tolerance," International Journal of Information Security, vol. 13, no. 4, pp. 367-390, 2014.

[55] T.R. Peltier, "Information Security Risk Analysis," Auerbach Publications, 2001.

[56] C. C. Lo and W. J. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls," Expert Systems with Applications, vol. 39, no. 1, pp. 247-257, 2012.

[57] Y. Deng, R. Sadiq, W. Jiang, S. Tesfamariam, "Risk analysis in a linguistic environment: a fuzzy evidential reasoning-based approach," Expert Systems with Applications, vol. 38, no. 12, pp. 15438-15446, 2011.

[58] S. B. Guarro, "Principles and procedures of the LRAM approach to information systems risk analysis and management," Computers & Security, vol. 6, pp. 493-504, 1987.

[59] J. A. Jones, "An Introduction to Factor Analysis of Information Risk (FAIR)," http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf, 2005, [Accessed January 2014].

[60] Riskwatch, http://www.riskwatch.com, 2005.

[61] NIST, "NIST SP - 800-53 rev3," 2009. [Online]. Available: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=903280. [Accessed March 2014].

[62] ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012.

[63] D. Ionita, "Current established Risk Assessment methodologies and tools," MSc thesis 2013.

[64] B. C. Guan, C. C. Lo, P. Wang, and J. S. Hwang, "Evaluation of information security related risks of an organization the application of the multi-criteria decision-making method," in Proceedings of the 37th IEEE Annual International Carnahan Conference on Security Technology, pp. 168-175, October 2003.

[65] S. Kondakci, "A composite network security assessment," in Proceedings of the 4th International Conference on Information Assurance and Security, pp. 249-254, IEEE Computer Society, 2008.

[66] A. Munteanu, D. Fotache, and O. Dospinescu, "Information systems security risk assessment: Harmonization with international accounting standards," International Conference on Computational Intelligence for Modelling Control & Automation, pp. 1111-1117, 2008.

[67] T. Alpcan and N. Bambos, "Modeling dependencies in security risk management," in CRiSIS. IEEE, 2009.

[68] J. Letchford and Y. Vorobeychik, "Computing optimal security strategies for interdependent assets," In Twenty-Eighth Conference on Uncertainty in Artificial Intelligence, 2012.

[69] R. E. Sawilla and X. Ou, "Identifying critical attack assets in dependency attack graphs," in 13th European Symposium on Research in Computer Security (ESORICS), pp. 18-34, 2008.

[70] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," Journal of Information Security and Applications, vol. 18, no. 1, pp. 45-52, 2013.

[71] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method," Computers & Security, vol. 24, no. 2, pp. 147-159, 2005.

[72] International Organization for Standardization, ISO/IEC 27005:2011. Information security risk management.

[73] Z. Wang and H. Zeng, "Study on the risk assessment quantitative method of information security," In 3rd International Conference on Advanced Computer Theory and Engineering, pp. 529-533, 2010.

[74] A. J. A. Wang, "Information security models and metrics," In Proceedings of the 43rd annual Southeast regional conference, pp. 178-184, 2005.

[75] S. H. Houmb, V. N. Franqueira, and E. A. Engum, "Quantifying security risk level from CVSS estimates of frequency and impact," Journal of Systems and Software, vol. 83, no. 9, pp. 1622-1634, 2010.

[76] P. R. Spencer, "Valuing Information Assets for Security Risk Management", Information Systems Security, vol. 9, no. 4, pp. I -7, 2000.

[77] K. Khanmohammadi and S. H. Houmb, "Business Process-based Information Security Risk Assessment," In 4th International Conference on Network and System Security, pp. 199-206, 2010.

[78] A. Shameli-Sendi, N. Ezzati-Jivan, M. Jabbarifar, and M. Dagenais, "Intrusion Response Systems: Survey and Taxonomy," International Journal of Computer Science and Network Security, vol. 12, no. 1, pp. 1-14, 2012.

[79] X. Su, D. Bolzoni, P. van Eck, and R. Wieringa, "A Business Goal Driven Approach for Understanding and Specifying Information Security Requirements," arXiv preprint cs/0603129, 2006.

[80] J. Eom, S. Park, Y. Han, and T. Chung, "Risk Assessment Method Based on Business Process-Oriented Asset for Information System Security," In Computational ScienceICCS, pp. 1024-1031, 2007.

[81] Y. Danfeng, Y. Fangchun, and L. Yu, "Service-based quantitative calculation of risk for NGN," In 2nd IEEE International Conference on Broadband Network & Multimedia Technology, pp. 306-310, 2009.

[82] G. Granadillo, M. Belhaouane, H. Debar, and G. Jacob, G. "RORI-based countermeasure selection using the OrBAC formalism," International Journal of Information Security, vol. 13, no. 1, pp. 63-79, 2013.

[83] M. Schmidt, "Return on investment (ROI) definition, meaning and use, encyclopedia of business terms and methods," http://www.business-case-analysis.com/return-on-investment. [Accessed March 2014]

[84] C. Duan and J. Cleland-Huang, "Automated safeguard selection strategies," CTI Research Symposium, 2006.

[85] W. Sonnenreich, J. Albanese, and B. Stout, "Return On Security Investment (ROSI). A Practical Quantitative Model," Journal of Research & Practice in Information Technology, vol. 38, no. 1, 2006.

[86] B. Mahmoud, N. Larrieu, and A. Pirovano, "A Risk Propagation Based Quantitative Assessment Methodology for Network Security-Aeronautical Network Case Study," In IEEE Conference on Network and Information Systems Security (SAR-SSI), pp. 1-9, 2011.

[87] I. Loloei, H. R. Shahriari, and A. Sadeghi, "A model for asset valuation in security risk analysis regarding assets' dependencies," In 20th Iranian Conference on Electrical Engineering (ICEE), pp. 763-768, 2012.

[88] M. Jahnke, C. Thul, and P. Martini, "Graph-based Metrics for Intrusion Response Measures in Computer Networks," Proceedings of the 3rd LCN Workshop on Network Security. Held in conjunction with the 32nd IEEE Conference on Local Computer Networks (LCN), pp. 1035-1042, Dublin, Ireland, 2007.

[89] N. Kheir, N. Cuppens-Boulahia, F. Cuppens, and H. Debar, "A service dependency model for cost sensitive intrusion response," Proceedings of the 15th European Conference on Research in Computer Security, pp. 626-642, 2010.

[90] L. Beaudoin and P. Eng, "Asset Valuation Technique for Network Management and Security", In Sixth IEEE International Conference on Data Mining-Workshops, pp. 718-721, 2006.

[91] F. Innerhofer-Oberperfler and R. Breu, "Using an enterprise architecture for IT risk management", Proceedings of the ISSA 2006 conference, 2006.

[92] B. Suh and I. Han, "The IS risk analysis based on a business model", Information & Management, vol. 41, no. 2, pp. 149-158, 2003.

[93] C. Samantra, S. Datta, and S. S. Mahapatra, "Risk assessment in IT outsourcing using fuzzy decision-making approach: An Indian perspective," Expert Systems with Applications, vol. 41, no. 8, pp. 4010-4022, 2014 Chicago

[94] A. Shameli-Sendi, M. Cheriet, A. Hamou-Lhadj, "Taxonomy of intrusion risk assessment and response system," Computers & Security, vol. 45, pp. 1-16, 2014.

[95] S. Schmidt and S. Albayrak, "A quantitative framework for dependency-aware organizational IT Risk Management," In 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp. 1207-1212, 2010.

Alireza Shameli-Sendi received his B.Sc. and M.Sc. with honors from Amirkabir University of Technology (Tehran Polytechnic). He received his Ph.D degree in computer engineering from Ecole Polytechnique de Montreal, Montreal, Canada. He is currently doing PostDoc at McGill in collaboration with Ericsson Research Security (Montreal, Canada) with the aim to develop a new security defense framework in cloud computing. His primary research interests include information security, vulnerability analysis, intrusion response system, and cloud computing. He is a recipient of Postdoctoral Research Fellowship Award from Canada (FQRNT).

Rouzbeh Aghababaei-Barzegar received his B.Sc. degree in Information Systems and Management from the University of London, London School of Economics and Political Science, United Kingdom. He has been working as an information security and IT service management consultant for several years. He is currently working as a member of the Information Security Framework Management Team at Ernst & Young GmbH, implementing and integrating various information security standards and frameworks. His research interests include information security risk assessment, IT service management, and vulnerability analysis.

Mohamed Cheriet received his M.Sc. and Ph.D. degrees in Computer Science from the University of Pierre et Marie Curie (Paris VI) in 1985 and 1988 respectively. Dr. Cheriet is expert in cloud computing and network virtualization. In addition, he is an expert in Computational Intelligence, Pattern Recognition, Mathematical Modeling for Image Processing, Cognitive and Machine Learning approaches and Perception. Dr. Cheriet has published more than 300 technical papers in the field. He holds Canada Research Chair Tier 1 on Sustainable Smart Eco-Cloud.