QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security

Prasad Saripalli
Runaware Inc.
Coral Springs, FL, USA
prasadsa@runaware.com

Ben Walters
Runaware Inc.
Coral Springs, FL, USA
ben@runaware.com

***Abstract*: A quantitative risk and impact assessment framework (QUIRC) is presented, to assess the security risks associated with cloud computing platforms. This framework, called QUIRC, defines risk as a combination of the Probability of a security threat event and it's Severity, measured as its Impact. Six key Security Objectives (SO) are identified for cloud platforms, and it is proposed that most of the typical attack vectors and events map to one of these six categories. Wide-band Delphi method is proposed as a scientific means to collect the information necessary for assessing security risks. Risk assessment knowledgebases could be developed specific to each industry vertical, which then serve as inputs for security risk assessment of cloud computing platforms. QUIRC's key advantage is its fully quantitative and iterative convergence approach, which enables stakeholders to comparatively assess the relative robustness of different cloud vendor offerings and approaches in a defensible manner.**

Keywords: Cloud Computing; Security; STRIDE; Risk; Impact; Delphi Method; Risk Asessment; CIAMAU

I. INTRODUCTION

Top industry analysts such as the IDC predict that cloud-based infrastructures will lead to major, transformational changes across the industry, and 2010 would be the tipping point. Several industry analysts and IT leaders are in agreement that cloud computing is poised to be a significant growth area. Modern cloud platforms hold a great promise to offer computing and IT as a cheaper and convenient service to the Enterprise and SMBs. The many advantages of cloud computing model, such as economy of scale, consolidation, efficiency in configuration and management, high availability and energy savings, are well documented [1-3]. The on-demand and pay-per-use model of cloud computing is expected to help IT achieve better utilization and help the enterprise avoid the costs of resource over-provisioning. It would also allow the enterprises, especially the medium organizations (MORG) and SMBs, to outsource IT setup and management, which typically are not their core expertise, and focus more on their business area [2].

At the same time, some key concerns have also emerged about cloud computing, which currently are viewed as significant barriers to its fast and wide-spread adoption. According to an IDC survey of CIOs consecutively in 2008 and 2009, security, integration and reliable performance ranked among the top concerns expressed [4]. An ENISA (European Network and Security Administartion) survey of Small and Medium Business (SMBs) also confirms that major concerns for SMBs migrating to the cloud include the confidentiality of their information and liability for incidents involving the infrastructure. [5]

This is understandable, because each of these factors have a major influence on the enterprises bottom-line. The Enterprise and SMBs today comprise of legacy systems and platforms, and legacy applications of significant complexity. This represents a major financial and engineering investment in the industry. Incompatibility of legacy systems and applications and inability of the new platform to integrate well with the existing infrastructures typically is a major blocker to the adoption of new technology. Similarly, availability of the platform with good performance and a satisfactory User Experience (UX) is the key differentiating factor among competing software products and services. UX provided by the SaaS model depends heavily on the quality of network characteristics, especially the roundtrip delay or latency [6]. Security is a key concern, because confidentiality, integrity, authenticity and auditability of business data, tools and transactions are critical requirements for businesses to stay functional, legal and competitive. This need is especially critical for certain business verticals such as Banking, HR, Security administration, Law Enforcement and Legal, for example.

In this paper, we present a quantitative framework for analyzing and assessing the risks and impacts to the security of cloud-based software deployments, and elucidate the advantages of such an approach. The rest of this paper is organized as follows. We present the security considerations for cloud platforms and the current thinking, based on security objectives. We then introduce the methods of risk assessment based on probability and impact, and the QUIRC framework. We demonstrate how the traditional Threat Modeling can be related to the QUIRC computations, via the identification of threat events. Using available data from The SANS Institute [7], we demonstrate the application of QUIRC to typical cloud deployment. We then present an approach to build more reliable input data for QUIRC analysis based on industry verticals and expert knowledge. Wide-band Delphi method is proposed as a suitable process for collecting such input from expert consensus. Merits and limitations of the proposed methodology are discussed.

978-0-7695-4130-3/10 $26.00 © 2010 IEEE
DOI 10.1109/CLOUD.2010.22

II. CLOUD SECURITY CONSIDERATIONS

There are multiple aspects to security requirements of enterprise workflows, which are well-documented in the literature [3, 7, 8], especially in the context of network security and the Internet. In response to the U. S. Federal Information Security Management Act (FISMA) of 2002, the Federal Information Processing Standards (FIPS) proposed confidentiality, integrity, availability, authenticity and accountability as the key principles of information security. Further, proportionality as a security principle implies that security controls should be proportional to the risks of modification, denial of use, or disclosure of the information. [8]

In this paper, we use the FIPS approach as a conceptual basis, and proportionality as represented by the Impact measure (I_e) of a threat event e and it's Probability of occurrence (P_e) as the quantitative basis for assessing security risks on cloud platforms. This approach also allows categorization of the security risks and impacts by Security Objectives (SO) as well as business verticals and functions. The U. S. Federal government follows a similar approach to set standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. Accordingly, FIPS provided guidelines recommending the types of information and information systems to be included in each category. These categories, called Security Objectives (SO) were set based on the potential impact on an organization when faced with attack events which may jeopardize the information and information systems. Such impact is assessed in terms of the organization's ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. FIPS recommended that the security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

FISMA [8] defines three security objectives for information and information systems, as Confidentiality, Integrity and Availability. Confidentiality is defined as "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]. A loss of confidentiality is the unauthorized disclosure of information. Integrity is defined as "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]. A loss of integrity is the unauthorized modification or destruction of information. Availability is defined as "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]. A loss of availability is the disruption of access to or use of information or an information system.

Chen et al. [9] recently visited the issues surrounding cloud platforms' security, and concluded that only few of the security issues are new and unique to cloud platforms, whereas the majority have been investigated and addressed in the context of traditional network and systems security [10, 11]. They identified multi-party trust considerations and mutual auditability as the two requirements unique to cloud platforms. We propose the addition of 3 more security objectives in the context of cloud platforms: Multi-party Trust, Mutual Auditability and Usability. Usability is explicitly included because overly aggressive security hardening, while helping the other 5 SO, could degrade the UX to a point where users may not like to use the platform. These 6 Security Objectives for the cloud platforms may be referred to as the CIAMAU framework. We present more complete details on the same in a following section.

III. THREAT MODELING

In information security, a threat represents a potential violation of the security of a system with some negative impact [10, 11], whereas vulnerability is an actual security flaw which makes a system susceptible to an attack. An attack is an exploitation of a vulnerability to realize a threat. Countermeasures are defensive architectural and implementation mechanisms used for mitigating vulnerabilities. Threat modeling for cloud platforms can help identify the threat events, their attack surface and the entry or access points on cloud assets in the context of each threat; analyze the threats and associated risks; and developing mitigating strategies.

Microsoft's STRIDE is a popular threat modeling approach, which identifies threats as shown in Table 1. Identifying and classifying the threat events helps in the assessment of their impacts and mitigation measures. STRIDE may be considered an alternative to the Security Objectives based CIAMAU categorization. For the purposes of QUIRC analysis, any one such categorization is sufficient. For completeness, we have categorized the STRIDE threat events to map to one or more of the 6 Security Objectives (SO) from Table 1, shown within square brackets [ ]. This is not an exact correspondence between the STRIDE and CIAMAU frameworks. While STRIDE is a well-tested framework for traditional software systems, a framework such as the CIAMAU presented here, which explicitly includes the cloud-specific Security Objectives, would be more appropriate for cloud security risk assessment. Security architects may also device their own alternative SO frameworks. QUIRC methodology would work with any such framework, by assigning relative weights of importance to each SO category, as will be shown later.

Table 1. Correspondence between STRIDE and SO models

THREAT	EXAMPLE
Spoofing: adversary poses as a user or entity with an identity. [CONFIDENTIALITY]	Illegally using another user's authentication information, such as username and password.
Tampering: modification of data to achieve a malicious goal. [INTEGRITY]	Unauthorized changes to persistent data, or alteration of data over a network.
Repudiation: ability to deny a malicious action lacking proof. [AUDITABILITY]	User performs an illegal operation in a system that lacks the ability to trace it.
Information Disclosure: exposure of protected data to adversary. [CONFIDENTIALITY]	A cloud user reads a file from a co-tenant's workflow, without permission.
Denial of Service: adversary gains a higher trust level and attacks. [AVAILABILITY]	An adversary gains control of a tenant's VM, and makes another's Web server unavailable.
Elevation of Privilege: unprivileged user gains privileged access. [CONFIDENTIALITY]	An attacker penetrates all system defense to join the trusted system itself

Common threats and attack patterns on cloud platforms can be documented in threat event catalogs, as shown in Lists 1 and 2 below. List 1 is compiled from recent literature on cloud security issues [12], whereas List 2 is drawn based on top 10 security threats listed for web applications [13] and Web 2.0 systems [14]. These lists may be expanded further as our understanding of cloud deployments evolves. Each item here would correspond to a threat event e, used in the QUIRC analysis.

List 1. Threat events compromising cloud security

1. **Resource Exhaustion:** Over or under provisioning of cloud resources leads to inadequate service or denial.
2. **Isolation Failure:** Failure in effectively separating storage, memory and routing causes isolation failure.
3. **Cloud Provider Malicious Insider:** a cloud provider's employee maliciously alters or corrupts customer data.
4. **Management Interface Compromise:** remote access and browser vulnerabilities while using customer management consoles of the cloud provider.
5. **Intercepting data in Transit:** failure in cryptographic techniques leads to data sniffing, spoofing and man-in-the middle attacks during transit.
6. **Data Leakage on Up/Down:** interception of data between the customer and the cloud provider leads to leakage of data to the third parties.
7. **Insecure or Ineffective Deletion of data:** improper deletion of data with a previous provider while migrating to a new provider.
8. **Distributed Denial of Service:** the attacker may use up all the metered resources of the customer.
9. **Economic Denial of Service:** malicious usage of customer resources may destroy economic value.
10. **Loss of Encryption Keys:** disclosure of secret keys of the customer to malicious parties.
11. **Undertaking malicious probes or scans:** malicious probes or scans on the customer resources.
12. **Compromise service engine:** core of the cloud i.e. service engine (e.g. hypervisor) has vulnerabilities.
13. **Conflicts between customer hardening procedures and cloud environment:** customers with vulnerable client environments join to increase the attack surface.

List 2. Threat events compromising Internet security

1. **Cross site Scripting (XSS):** script executes in victims browser to hijack user sessions, deface web sites, and introduce worms etc.
2. **Injection Flaws:** user data sent to the web application is not properly validated, which can manipulate a query on the server.
3. **Malicious File Execution:** PHP, XML or any other framework which accept a file from the user is vulnerable to this attack, as the file can contain a malicious script.
4. **Insecure Direct Object Reference:** direct reference to any internal implementation object such as file, database record, key etc can be exploited.
5. **Cross-site Request Forgery:** a logged on user's pre-authenticated data of a web site can be exploited by attacker's application when he visits his site.
6. **Information Leakage by Improper Error Handling:** attack on the applications to sniff information on system resources, working and configuration.
7. **Broken Authentication and Session Management:** attack on account credentials and session tokens which are not protected.
8. **Insecure Cryptographic Storage:** web applications which do not use cryptographic functions to protect the data are exploited.
9. **Insecure Communication:** failing to encrypt the network traffic leads to this attack.
10. **Failure to restrict URL Access: p**revention of access by not displaying the urls to unauthorized users can be exploited by direct access of urls.
11. **XML poisoning:** XML traffic between the server and the browser is poisoned.
12. **Malicious AJAX Code Execution:** malicious AJAX code in the web application silently executes attacker's intent.

13. **RSS/Atom Injection:** RSS feeds are injected with literal Java Script that can generate attacks on client's browser.
14. **WSDL Scanning and Enumeration:** WSDL (Web Services Definition Language) file is attacked.
15. **Client side validation in AJAX routines:** same as 2 in the above section.
16. **Web Services Routing Issues:** unencrypted SOAP messages in WS Routing leads to this attack.
17. **Parameter Manipulation with SOAP:** attacker manipulates the variables in the SOAP messages.
18. **XPATH Injection in the SOAP Messages:** XPATH statements which take user input are manipulated.
19. **RIA Thick Client Binary Manipulation:** RIA components such as the Flash, Active X Controls and applets downloaded as binary components are decompiled to obtain the code. Applying patches to these binaries can bypass security.

IV. SECURITY RISK ASSESSMENT

Gartner [14] provided a basic description of the potential risks involved with cloud computing. Cloud Cube Model [15] was proposed as a framework to understand the organizational perimeters and associated privilege policies for information in different types of clouds. European Network and Information Security Agency (ENISA) provided a detailed description of the issues and requirements for cloud security. This report's key conclusion was that the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective.

The ENISA report [4] also provided an approach for risk assessment based the estimation of risk levels on ISO/IEC 27005:2008. Security risk would be high if both the probability of the event and its impact are high. Risks are categorized into three groups: policy and organizational risks, technical risks and legal risks. The assessment provided is semi-quantitative, as it uses value ranges for both event probability and impact, but does not consider their combined influence in a quantitative manner. Instead, the final risk assignment (as High, Medium or Low) is based on expert opinion, which takes the two factors into consideration. For example, risk due to vendor lock in is assessed to be High, because its probability is high, but impact is Medium. Loss of Governance is shown as a risk with both high probability and high impact, and hence a 'very high risk'. A fully quantitative risk assessment framework would further improve this methodology, because it enables the stakeholders to comparatively evaluate the risks involved and protection measures. Several other application domains, such as nuclear power, public health and environmental planning, employ such fully quantitative frameworks [17].

A. Quantitative Risk Assessment

Following the earlier work of Saripalli et al. [17], we propose a definition for risk as a product of the Probability (P_e) of a security compromise, i.e. a threat event, e, occurring and its potential Impact or Consequence (I_e):

$$R_e = P_e I_e \qquad (1)$$

P_e typically is a fraction less than 1, whereas I_e may be assigned a value on a numerical scale. In this study, we propose these ranges for Impact (I_e): LOW (1-5); MODERATE (6-10); HIGH (11-15). These values are relative, and may be amplified depending on the required granularity for the visualization of risk metrics.

Following the FIPS model [7], we propose the following impact definitions for the security of cloud platforms. The potential impact is LOW if the loss of confidentiality, integrity, availability, mutual trust or mutual auditability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. For example, such an impact could (i) cause degradation in business capability to an extent and duration that the organization is still able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. In the context of cloud computing, an organization may be defined as any business unit participating directly as a tenant on a given cloud platform, including end customers who use the cloud services.

The potential impact is MODERATE if loss of confidentiality, integrity, availability, mutual trust or mutual auditability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the above loss might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law. The potential impact is HIGH if the loss of confidentiality, integrity, availability, mutual trust or mutual auditability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss might: (i) cause a severe degradation in or loss of business capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. These definitions are based heavily on the FIPS descriptions, with appropriate modifications for the cloud applications.

V. IMPACT (CONSEQUENCE) ASSESSMENT

Establishing an appropriate SO for each threat event requires determining its potential impact first. FIPSA proposed a generalized format for expressing the security category, SC, of an information type as:

$SC = \{(\text{CONFIDENTIALITY}, \text{I}), (\text{INTEGRITY}, \text{I}), (\text{AVAILABILITY}, \text{I})\}$

Acceptable values for potential impact (I) are LOW, MODERATE, HIGH, or NOT APPLICABLE. Here, I refers to an SO category and not an actual threat event.

Such SC description is not amenable for developing quantitative risk or impact metrics, as the formula above is meant for categorization only. In the present study, such quantitative basis is developed, referring the Impact to a specific security event, *e*. Several examples are presented in the following discussion, illustrating how to calculate the Impact index (I_E), for typical cloud deployment examples.

As an initial example, consider an organization managing public information on its web server (e.g. a Public Library Catalog) experiencing DoS attacks. The library determines that there is no potential impact from a loss of confidentiality (*i.e.*, confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. Multi-trust and Auditability criteria are low priority in this event, whereas usability would have a moderate impact. The resulting I_e would be a six tuple for CIAMAU, as below:

I_e = [(C, 0), (I, 6), (A, 8), (M, 1), (A, 1), (U, 8)]

Thus, Impact always corresponds to a specific threat event *e*, which maps to one of the 6 Security Objectives (SO) and/or an alternative categorization such as STRIDE. In this approach, LOW impact implies a **limited** adverse effect on organizational operations, organizational assets, business outcomes or individuals, due to a breach in any of the 6 SO. MEDIUM impact implies a **serious** adverse effect, and HIGH impact implies a **severe or catastrophic** adverse effect, on the four criteria described. Further examples of Impact based on CIAMAU are presented in Table 2.

Impact tables can be prepared for various threat events, to assess security risks for a particular class of customers (i.e., a vertical) considering the potential consequences as provided by Subject Matter Experts (SME). SME are not security experts, but are knowledgeable about the impact of threats on their particular type of business. Wide Band Delphi analysis presented in a later section can be used, to generate consensus estimate for Impact values among an SME team.

Risk is a combination of the probability, or frequency, of a security threat event and the magnitude of its consequence, usually their product [17]. After the experts converge on a consensus for these values, security risk under each CIAMAU category is assessed as per Eqn. (1), and the overall platform security risk for the given application under a given category (R_s) would be average over the cumulative, weighted sum of *n* threats which map to that SO category:

$$R_s = \frac{1}{n}\sum_{i=1}^{n} P_e I_e \qquad (2)$$

For example, if there are 3 threat events identified under Integrity, with the I_e values of {3, 7, 11}, and their probabilities of occurrence are {0.01, 0.001 and 0.004}, then the Risk value under the Availability SO would be [0.01(3) + 0.001(7) + 0.004(11)] or 2.431. It is also necessary to assign a weight for each of the SO categories, such that their sum always adds up to 1. This weight, w_s, represents the relative importance of a given SO to a particular organization and/or business vertical.

Then, Net Security Risk (R) to the application integrated over the six CIAMAU objectives is a weighted average:

$$R = \sum_{s=1}^{6} w_s R_s \qquad (3)$$

where w_s is the relative weight assigned to an SO category *s*. For example, consider an entertainment content portal, which has world-wide operations with several fierce competitors, some of whom are served (as co-tenants) on the same cloud vendor's platform. Confidentiality and Integrity of entertainment content are not critical, but availability, usability, auditability and multi-tenant trust would be important in that order. A CIAMAU tuple for w_s as [0, 0.1, 0.4, 0.2, 0.1, 0.3] captures these priorities well. I this example, suppose the actual risks (R_s) due to all threat events pooled under each CIAMAU category are [11.2, 13.1, 3.3, 2.8, 4.1, 7.4]. Then, Net Security Risk on the cloud platform equals their weighted sum, 2.37, per Eqn. 3.

Evaluation of the probabilities of several threat events currently is difficult, due to a lack of historic data. For example, in the case of spoofing attacks, critical data need is the frequency of occurrence of such attacks globally on ALL enterprise systems. While such data are not readily available, collaborative research among institutions

analyzing security data will be very helpful to collect the same. In the next section, we present one such data source, from the SANS institute [7].

Just as the Impact (I_e) is a function on specific threat events, the event's Probability (P_e) also is a function of specific threat events. As such, it is necessary to provide a compilation of all plausible threat events on cloud platforms. The compilation presented in Lists 2 and 3 can be further expanded, as research into cloud security issues reveals further threats. Each such threat can be mapped to one of the six CIAMAU, and assigned I_e and P_e values. This is best done by SMEs considering the industry vertical and the specific scenarios in which the cloud application is deployed. Once these values are assessed realistically, risks can be assigned to the platform as a whole.

All such threat events would be mapped to one or more of the CIAMAU categories. Occasionally, a threat may contribute to breaches in more than one of the security objectives. For example, a spoofing attack which allows an intruder to access a tenant's VM images and launch an attack to deny services from a neighboring tenant on the cloud platform would represent a threat to Integrity, Confidentiality as well as Multi-trust. The QUIRC framework allows filing such threat events under multiple SO categories. This does not lead to any duplicity in risk calculations because the weights w_s will suitably divide the influence of a threat event on multiple SO.

Table 2. Examples of Impact of threat events on security

SECURITY OBJECTIVE	IMPACT EXAMPLE
Confidentiality (illicit information disclosure.)	A scholastic test's contents leak by sniffing prior to test date [9]
Integrity (unauthorized information alteration)	A news archival store's backup images corrupted by intrusion [3]
Availability (access disruption to systems.)	VM allocation for a tenant fails to meet sudden surge in sales [8]
Multi-Trust (breach of SLA of one tenant due to another's actions.)	A VM containing a stock trader SMB's data stolen by a co-tenant and used for illicit trading [9]
Auditability (lack or compromised auditable record of usage.)	Audit trails for a tenant's workflows are lost for 2 days in an year but no issues surface [2]
Usability (degraded UX for a tenant.)	Intruder scripts randomly display on a video subscription portal [4]

For example, for a business in the Banking sector, Integrity could be a paramount SO, because any tampering of financial data would have severe consequences. In contrast, at a private security agency, Confidentiality may be the most critical. Subject Matter Experts (SME) from the particular verticals would be able to define the weight values as well, for a given business vertical. The I_e and P_e values presented in this paper are intended only for illustration purposes. These values should not be used for planning actual cloud deployments, without SME verification.

VI. PROBABILITY ASSESSMENT

SANS Institute recently provided a comprehensive dataset and analysis on Internet security vulnerabilities, covering existing and emerging threats that pose significant risk to networks, focusing on those threats that have the greatest potential to negatively impact the Enterprise [7]. This report serves as an excellent example for the calculation of threat probabilities described here. Internet serves as a good surrogate for the vulnerabilities and threats to be expected on cloud computing platforms, because cloud essentially depends on the Internet for its functioning. According to the SANS report [7], attacks against web applications constitute more than 60% of the total attack attempts observed on the Internet, mainly focused on converting trusted web sites into malicious websites serving content that contain client-side exploits. Web application vulnerabilities such as SQL injection and Cross-Site scripting flaws in open-source as well as custom-built applications account for more than 80% of the vulnerabilities being discovered. SANS team collected over 6 months March 2009 to August 2009 - from appliances and software in thousands of targeted organizations to provide a reliable portrait of the attacks being launched and the vulnerabilities they exploit.

Data on actual attacks came from intrusion prevention appliances that protect more than 6,000 companies and government agencies. Data on vulnerabilities that remain unpatched came from appliances and software deployed by Qualys that monitor vulnerabilities and configuration errors in more than 9,000,000 systems, scanned more than 100,000,000 times 2009. SANS identified the four major attack categories as high-risk threats to most if not all networks, as the Server-Side HTTP attacks, Client-Side HTTP attacks, PHP Remote File Include, Cross-site Scripting attacks, and finally SQL Injection attacks. United States United States was found to be the major attack target for the Server-Side HTTP attack category.

To calculate an event P_e, if it is assumed that a given server system is accessed 1000 times for SQL queries during a day, then, over a 6 months period of time across the 9,000,000 systems studied in the SAN study, there were a total of 1,620,000,000,000 SQL transactions. Among them, 250,000,000 were actual SQL injection attacks, indicating that the probability of this type of attacks is 0.00015. Using this approach, probabilities of occurrence (Table 3) were calculated for 4 major threats on Enterprise Internet systems, using the data from [7]. These numbers are for illustration purposes only, because a key piece of information – the actual number of times the server (or web application) sessions were accessed in a day was an

assumed value (1000) and needs to be validated. However, this analysis shows a basis to develop a fully quantitative methodology the security risk assessment of clouds.

Table 3. Example event probability calculations

Attack type (e)	#of events reported	# transactions per day*	P_e
SQL Injection attack	250000000	1000	0.00015
Server-Side HTTP attack	8200000	500 (server access)	0.00001
PHP Remote file include	2200000	200 (File access)	0.7e-06
Cross-site Scripting	2700	100 (Scripts run)	1.6e-07

* Number of transactions per day is an assumed number and not actual measured data.

A comprehensive compilation (Threat Catalog [11]) needs to be developed for all relevant events such as shown in Lists 3 and 4, as number of events/year for a given type of security compromise event. A more accurate assessment of probabilities will be business and application specific, based on characterization data from actual incidence of security compromise events. Once the probability of occurrence of all such events is calculated, risk (R) can be calculated as explained. Such calculations are useful in identifying the high-risk threats, and investigating them in greater detail.

VII. WIDE-BAND DELPHI METHOD

A widely accepted method for the evaluation of impacts based on expert opinion is the Wide-band Delphi method, using rankings based on expert opinion about the likelihood and consequence of threats [18]. The Delphi method is a forecasting technique used to collect expert opinion in an objective way, and arrive at consensus conclusions based on that. It was developed by the RAND Corporation in the 1950's and 1960's [18-20] for gathering a knowledge base of military intelligence and experience, without the influence of politics, rank, or other bias. It has since been applied to other domains such as technology, population sciences, usability studies, environmental risk assessment and business applications.

In this method, a moderator is used to control and facilitate information gathering from a selected group of SME. Three essential characteristics of this method are structured and iterative information flow, anonymity of the participants and iterative feedback to the participants.

During the Delphi process, each participant is asked to provide an answer to a problem or question, such as the Impact of a particular threat event and map it to one of the 6 SO. A questionnaire is designed such that the participant can easily provide a numerical answer to the questions. Following this step, the moderator merges the answers from all the participants in an anonymous presentation and shares that combined result with all the participants.

The participants are then allowed and encouraged to reconsider and modify their answer after review of the previous work. Throughout the process, the moderator is encouraged to filter any bias and provide relevant personal opinion or experience. While this direct interaction of the moderator facilitates communication among the participants and facilitates the process towards consensus, it was also noted as one of the weaknesses in the method [22]. The moderator should maintain an objective view of the information and remain neutral on any presented positions. To avoid any potential conflict of interest, unbiased, third-party moderators may be used for critical evaluations. Independent verification and validation is one such method used in the development of mission critical systems [23-25].

The Delphi method has unique benefits over other group communication methods [21]. Instead of direct collaboration, Subject Matter Experts (SME) interact through an iterative synthesis which does capture all of their inputs, while allowing all participants to iteratively revise their opinions and inputs in light of the rest of the discussion. The opinions of others can be influential, valuable, insightful, or useless depending on the context and the particular SME's expert views. This anonymous collaboration alleviates peer pressure and other performance anxieties that are common to group collaboration methods and allows participants to both assert and revise their views in a quantitative, iterative fashion.

Prior to conducting this process, the moderator needs to prepare a good overview of the cloud application's business goals, key scenarios, scope and assumptions. He or she also needs to have a list of all plausible threat events, and a mapping of each event to one of the six SO. Further, data on the Probability of occurrence of each event (P_e) should also be collected from earlier records and research, specific to the business and the geographical region, using sources such as [SAN report]. The pieces of information to collect from the Delphi process are (i) the relative weights (w_s) for each of the six SO for the given business application, the Impact (I_e) of each event as a numerical value, and the degree of confidence in the probability P_e.

A. The Wide Band Delphi Process

1. Select session moderator and SME participants.
2. Hold planning meeting and explain the goals, context and security goals of the cloud deployment.
3. SMEs individually provide their best numerical estimates for the impact of every listed event, weights and confidence in P_e values based on the questionnaire.

4. Moderator tabulates and compiles this data and shares results, including summary statistics with all involved.
5. Repeat step 3-4 to converge all data values within an acceptable range. (*e. g.* 10% variance).

Once a trained team is assembled to perform estimations, the moderator fills out the Project Information sheet in the tool. The moderator privately assigns each SME an ID number which should be kept private.

For steps 3 and 4 above, the SMEs communicate their estimates privately to the moderator, which the moderator types into a tool for the appropriate round and ID number. The summary results are displayed graphically to all at the end of the round. If the results are narrow enough to accept (step 5 above), the process is complete. Otherwise there is a round of discussion where the SME continue to discuss the results. Any new assumptions surfacing should be listed in the display tool. This process works in live meetings, and email, Internet and phone as well. The data so collected as expert consensus is fed to the QUIRC Risk calculations (Eqn. 1 – 3), to assess Risks by SO and the Net Risk.

A. Risk Mitigation and Prevention Measures

The quantitative approach presented here would naturally lead to a correlation of the security threat mitigation and prevention measures to the risk and impact metrics. Following the I^2SF (International Information Security Foundation) committee's recommendations on information security, a cloud platform's security may also be strengthened using a combination of preventive, detective, and recovery measures. In the context of a cloud platform, a preventive measure is a measure that avoids or deters the occurrence of an event which can compromise security. Passwords, federated identity management tools, keycards, badges, contingency plans, policies, firewalls, and encryption are examples of preventive measures. A detective measure is a risk control that identifies the occurrence of an undesirable event, after the fact. This is an important reason why auditability of the cloud platform is necessary. Visitor logs, audit trails, time stamps, analytic engines, motion sensors, closed-circuit TV, and security reviews are examples of detective controls. Reporting and additional analytics using such tools also helps both respond to and prevent the future occurrence of such events.

Design and implementation of a cloud platform to assure non-repudiation, pedigree tracking and provenance tracking of cloud entities and workflows further helps with both the prevention and detection of security compromises. Recovery measures such as redundancy, fault tolerance, backup and disaster recovery plans help restore the integrity, availability, and confidentiality of information assets to their expected state. As the cloud platforms evolve and mature, it is likely that new threat events and counter-measures would be developed. All such measures would have a 'negative Impact' value on the corresponding threat events, which can be substituted in Eqn. 3 and 4, to assess the improved (mitigated) risk under each SO and the entire application. This methodology would be helpful to decision makers, regulators and security architects as well, to comparatively evaluate the net value of security measures among different design approaches and across platforms.

VIII. CONCLUSIONS

A quantitative impact and risk assessment methodology for cloud computing projects is developed, to assess the security risks associated with cloud computing platforms. This framework, called QUIRC, uses the definition of risk as a combination of the probability of a security threat event and its severity, measured as its Impact. Six key security criteria are identified for cloud platforms, and it is shown that most of the typical attack vectors and events map under one of these six categories. A modified wide-band Delphi method is proposed as a scientific means to collect the information necessary for assessing security risks. Risk assessment expertise could be developed specific to each industry vertical, and a knowledge-bases could be generated, which then serve as objective bases for security risk assessment of cloud computing platforms.

Advantages of the QUIRC methodology are as follows. A quantitative approach gives vendors, customers and regulation agencies the ability to comparatively assess the relative robustness of different cloud vendor offerings and approaches in a defensible manner. It also can be helpful in alleviating the considerable FUD (Fear, Uncertainty and Doubt) associated with cloud platform security issues and helping that they are dealt in an effective way. For example, the high risk SOs and events would emerge which will then be addressed with counter measures. Limitations of the approach include that it requires the meticulous collection of input data for Probabilities of events, which requires collective industry SME inputs. Other industries such as environmental, nuclear and seismology and public health communities have successfully implemented such approaches however.

ACKNOWLEDGMENT

We are thankful to the security engineering teams at SAN, FIPS, ENISA and UC Berkeley, whose findings were helpful to our work, and Runaware Inc (R&D) for its sponsorship.

REFERENCES

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M.

2009. Above the Clouds: A Berkeley View of Cloud Computing. Technical Report. University of California at Berkeley.

[2] IDC Cloud Computing 2010 - An IDC Update, Frank Gens, Robert P Mahowald, Richard L Villars, Sep 2009 - Doc # TB20090929, 2009.

[3] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009, http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

[4] IDC Cloud Computing Survey http://blogs.idc.com/ie/?p=210 accessed on January 25, 2010.

[5] ENSIA Report on Cloud Computing Security Risk Assessment http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment (accessed on January 18th, 2010.)

[6] Saripalli, K.P., Oldenberg, C., Walters, B. and Radheshyam, N. (2010) A Cloud Architecture and Platform for Scientific Computing as a Service (SCaaS) ACM CloudScience2010 (in review).

[7] The Top Cyber Security Risks, SAN Institute Report (Sept. 2009) http://www.sans.org/top-cyber-security-risks/ accessed on January 18, 2010.

[8] Federal Information Processing Standards Pub 199: Standards for Security Categorization of Federal Information and Information Systems http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf accessed on Jan 7, 2010.

[9] Chen, Y., Paxson, V. and Katz, R. H. (2010) What's New About Cloud Computing Security? University of California, Berkeley Report No. UCB/EECS-2010-5 January 20, 2010 http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf accesed on February 18, 2010.

[10] Poore, R. S. (1999) International Information Security Foundation, Generally Accepted System Security Principles Release for Public Comment. www.infosectoday.com/Articles/gassp.pdf *accessed on January 11, 2010.*

[11] Elahi, G. and Yu, E. A Goal Oriented Approach for Modeling and Analyzing Security Trade-Offs; Lecture Notes in Computer Science Springer Berlin / Heidelberg Volume 4801/2007

[12] Ristenpart, T., Tromer, E., Hovav Shacham, H. and Stefan Savage, S. (2009) Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, CCS'09, Chicago, IL, USA.

[13] OWASP Top 10 Web Security Vulnerabilities (2007) accessed on January 11, 2010 http://www.owasp.org/index.php/Top_10_2007

[14] Web2.0 http://www.net-security.org/article.php?id=949&p=4

[15] Gartner, Assessing the Security Risks of Cloud Computing, June 2008, http://www.gartner.com/DisplayDocument?id=685308

[16] Forum, J. Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, April 2009, http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

[17] Saripalli, K.P., Mahasenan, N.M. and Cook, E.M., 2003. Risk and hazard assessment for projects involving the geological sequestration of CO2 In: Gale, J. and Y. Kaya (eds.) Sixth International Greenhouse Gas Control Conference, Kyoto, Japan, pp. 285–289. Elsevier Ltd. (2003).

[18] Linstone, H.A. (1975). The Delphi Method: Techniques and Applications. Addison-Wesley.

[19] RAND Corporation. (2007). A collection of RAND publications on the Delphi method. Accessed on Jan 15, 2010 from http://www.rand.org/pardee/pubs/methodologies.html#delphi.

[20] Stuter, L.M. (1996). The Delphi Technique: What is it?. Lynn's Educational and Research Network, March 1996. Retrieved from http://www.learnusa.com/transformation_process/acf001.htm .

[21] Paul, C. L. A Modified Delphi Approach to a New Card Sorting Methodology J. Usability Studies Vol. 4, Issue 1, November 2008, pp. 7-30

[22] Teijlingen, E., Pitchfork, E., Bishop, C., & Russell, E. (2005). Delphi method and nominal group techniques in family planning and reproductive health research. Journal of Family Planning and Reproductive Health Care, 31(2) 132-135.

[23] Paul, C.L. (2007). Investigation of Applying the Delphi Method to a New Card Sorting Technique. Information Architecture Institute, June 6, 2007. Accessed January 15, 2010, from http://iainstitute.org/news/000632.php.

[24] Whitmore, M., Berman, A., & Chmielewski, C. (1997, March). Independent Verification and Validation of Complex User Interfaces: A Human Factors Approach (TP-3665). Houston, TX: Lockheed Martin Engineering & Science Services.

[25] Nadeau, R., Cloutier, E., & Guay, J.H. (1993). New Evidence About the Existence of a Bandwagon Effect in the Opinion Formation Process. International Political Science Review, 4(2), 203-213.