2018

The Design and Evaluation of a User-Centric Information Security Risk Assessment and Response Framework

Alohali, M

10.14569/ijacsa.2018.091018
International Journal of Advanced Computer Science and Applications
The Science and Information Organization

The Design and Evaluation of a User-Centric Information Security Risk Assessment and Response Framework

Manal Alohali[1,2], Nathan Clarke[1,3], Steven Furnell[1,3,4]
[1]Centre for Security, Communications and Network Research, Plymouth University, United Kingdom
[2]College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Saudi Arabia
[3]Security Research Institute, Edith Cowan University, Western Australia
[4]Centre for Research in Information and Cyber Security, School of ICT, Nelson Mandela University, South Africa

***Abstract*—The risk of sensitive information disclosure and modification through the use of online services has increased considerably and may result in significant damage. As the management and assessment of such risks is a well-known discipline for organizations, it is a challenge for users from the general public. Users have difficulties in using, understanding and reacting to security-related threats. Moreover, users only try to protect themselves from risks salient to them. Motivated by the lack of risk assessment solutions and limited impact of awareness programs tailored for users of the general public, this paper aims to develop a structured approach to help in protecting users from threats and vulnerabilities and, thus, reducing the overall information security risks. By focusing on the user and that different users react differently to the same stimuli, the authors developed a user-centric risk assessment and response framework that assesses and communicates risk on both user and system level in an individualized, timely and continuous way. Three risk assessment models were proposed that depend on user-centric and behavior-related factors when calculating risk. This framework was evaluated using a scenario-based simulation of a number of users and results analyzed. The analysis demonstrated the effectiveness and feasibility of the proposed approach. Encouragingly, this analysis provided an indication that risk can be assessed differently for the same behavior based upon a number of user-centric and behavioral-related factors resulting in an individualized granular risk score/level. This granular risk assessment, provided a more insightful evaluation of both risk and response. The analysis of results was also useful in demonstrating how risk is not the same for all users and how the proposed model is effective in adapting to differences between users offering a novel approach to assessing information security risks.**

***Keywords*—Risk; analysis; security behavior; BFI; correlation**

I. INTRODUCTION

Given the rapid growth of technology and the wide range of 24/7 e-services provided by different devices such as laptops, mobile phones and wearable technology, the number of users is growing every day. With more than 3.8 billion Internet users in 2017 compared to 2.9 billion in 2014 [1] and one or more Internet-connected devices used in most homes [2], users massively use Information Technology (IT) systems to carry out their everyday activities. With this increased popularity of the Internet and its services, comes an increase in information security threats such as malware, social engineering and hacking that some users are arguably not aware of [3]. Despite the common use of various security methods such as intrusion detection systems and antivirus software to protect IT systems from different attacks, the security threat landscape is rapidly evolving and attackers are increasing their efforts in developing sophisticated and advanced malware and hacking methods. This is evident as the number of created malware grew from 274 million in 2014 to almost 670 million with a rate of 1.8 million threats introduced everyday in 2017 [4] and an email malware rate of 1 in 131in 2016 compared to 1 in 244 and 1 in 220 in 2014 and 2015 respectively [5]. Attackers have a higher chance of infecting a user's computing device with malware if it has at least one popular installed application that is vulnerable and out-of-date [6].

Managing and assessing information security risks in organizations is a well understood and accepted approach used widely by enterprise organizations to provide a safe environment to carry out their business using the most cost-efficient and effective means [7][8]. Many Information Security Risk Management (ISRM) methodologies were issued by National and International organizations such as The National Institute of Standards and Technologies (NIST) Special Publication 800-series [9] and The International Standards Organization ISO/IEC 27000 [10] or as research projects [11]. Unfortunately, these traditional risk assessment methodologies and tools are designed for organizations and not members of the public. Considering the increased number of Internet users, the variety of used devices where each device has its own security requirements and the continuously evolving threat landscape, the need for assessing information security risks is not limited to organizations only. Actually, this need is expanded to a wider population to include users from the general public or simply, users.

Unfortunately, little evidence is found demonstrating that users are knowledgeable of information security threats and protection, and actually practicing it [12][13][14]. Indeed, it has been found that they are less willing to perform money-related and sensitive data tasks on some of these devices such as smartphones due to issues related to security, privacy, trust and usability [15][16]. Furthermore, users have difficulties in

using, understanding and reacting to security-related threats [16][17][18]. Although educating users about information security threats is a well-established and accepted approach in organizations where resources are, arguably, allocated to achieve the organizations' goals, it is a challenge in the case of users [19]. Almost 90% of reported security incidents resulted from exploits against software vulnerabilities whereas human-error was considered as one of the top threats to information security and almost 1.8 million pieces of malware introduced every day [4][14][20][21]. Hence, the need for a usable security tool that calculates and assesses risk on both system and user level in a timely manner is essential. Additionally, the limited impact of awareness programs suggests the need for a structured approach tailored for users to help in protecting them from threats and vulnerabilities and, thus, reducing the overall information security risks [22]. By focusing on the user, increased security awareness through understanding risk is expected to improve security behavior and lead to reduced security risks [23]. Therefore, the aim of this paper is to develop a comprehensive and continuous framework that assesses and communicates information security risks for users of the public in both an individualized and timely manner.

The remainder of this paper is structured as follows: Section 2 reviews related work on assessing and communicating risks to users. Section 3 presents a user-centric framework to information security risk assessment and response. This proposed framework is evaluated in Section 4 followed by a discussion in Section 5. Finally, conclusions and future work are highlighted in Section 6.

II. Related Work

There are a large number of proposed ISRM methodologies and guidelines around the world that differ in their approach, level of detail, usage complexity and applicability to different-sized organizations [24][25]. There are various Information security standards by organizations such as ISO/IEC 27005:2011[10] and NIST SP 800-30 [9]. Additionally, various Risk Assessment (RA) methodologies were developed by professional organizations to meet specific requirements and therefore incorporate different steps, objectives, level of application and structure. Examples of such methodologies are CRAMM [26], CORAS [27], OCTAVE [28], Magerit [29] and Mehari [30] that have been fully or partially adopted by organizations to identify, analyze and treat their information security risks. Furthermore, these methodologies have different analysis approaches towards risk whether threat-oriented, Asset/Impact oriented or Vulnerability-oriented. They are quantitative, qualitative or semi-quantitative in nature where there is no exact risk value because of the uncertainty and subjectivity in defining likelihood and severity of consequences [31]. To reveal major risks and to get a general indication of the risk level, a quantitative estimation could be used first followed by a qualitative analysis. Among those techniques used to calculate information system's risks is Vulnerability Management that is represented by The Security Content Automation Protocol SCAP [32][33]. To communicate security information, SCAP provides several standard specifications, including Open Vulnerability and Assessment Language (OVAL) [34] ,Common Vulnerabilities and Exposure (CVE) [35] and Common Platform Enumeration (CPE) [36]. The Common Vulnerability Scoring System (CVSS) is a scoring system that provides a standard specification that measures the severity of software vulnerabilities [37] and a widely used cybersecurity model [21][32][33][38][39][40]. The National Vulnerability Database (NVD) is a valuable source of security knowledge and publically available online [41]. Each NVD record contains CVE-id, vulnerable software list, vulnerability published date and time, CVSS base metrics and scores and so on. NVD uses CVSS to measure vulnerabilities severity which provides evidence of the wide and accepted adoption of CVSS by the security community [42]. Moreover, it is often used as a metric for risk [38].

There are many proposed RA methodologies in the literature that are built on those methodologies where each method has its own objectives, steps, structure and level of application. Based on the OCTAVE methodology and in the context of educational organizations for example , authors of [43] proposed risk assessment framework for a university computing environment and [44] performed an ISRM study in order to educate management and users of a computer information system in secondary schools on how to protect their information assets and reduce risks to their information systems through risk management. In the former, the risk assessment proposed needed skilled individuals that understand statistics, probabilities and information technology. Whereas in the latter, given the conservative environment of schools, the observed behavior of the selected sample members maybe inaccurate with the presence of the researcher and may not reflect their actual normal behavior. Authors of [45] proposed a RA methodology for smartphones that has an ISO/IEC 27005:2011 compatible theoretical basis. The proposed risk assessment method provides "fined-grained" valuation. User input for (sub) asset impact is based on two-dimensional data taxonomy. This user involvement, leads to a 'personalized' risk assessment, where other smartphone oriented methods use mainly expert opinion. However, user input details vary according to user skill which may affect the quality of results. Also, users assessing the asset impact of application is complex where the number of applications maybe numerous and the user is assumed to know the applications significance. A risk management methodology was proposed in [46] based on NIST SP 800-30 risk management guide. However, the proposed methodology does not determine the exact interaction between controls and resource dependency nor evaluate the way in which threats spread through the system. Authors of [47] used a qualitative approach, structured interviews, to identify potential threats then a quantitative approach, survival analysis, to analyze the risks. A particular strength of this framework is that it considers the time dimension in identifying threats that vary over time. However, there could be difficulties with applying this framework in practice since it has not been tested yet, so no indications of its effectiveness and reliability.

To the author's knowledge, despite the increased attention on Information Security Risk Assessment (ISRA) in enterprise organizations, there is a lack of tools and methods in the literature that are tailored for the general public. Nevertheless,

some websites do provide information and advice on how to protect yourself in the cyber world such as Getsafeonline.org and staysafeonline.org. However, they could be used as awareness tools that provide advice and guidance to users to make informed decisions regarding their security behavior. These tools do not provide the expected level of RA that users are exposed to. Many of these users are not aware of these risks and/or do not have the necessary knowledge to use the available websites to analyze these risks and overcome security risks problem. A web-based risk analysis tool for home users based on the ISO 17799 standard was proposed by [48]. The performance of the tool was evaluated with means of the interface design described as user-friendly, easy to use and accessible. No evaluation regarding the way the tool assessed the different security levels and the provided support, maybe because it has not been tested by users with a certain level of security background. Authors of [49] proposed a Mobile Device Risk Assessment (MDRA) risk assessment method based on a 6-step risk calculation scheme. Although the proposed approach is clear and easy to use by different stakeholders, the whole risk calculation process was challenging for novice users. The framework proposed by [23] was a continuous and automated risk assessment framework for Android mobile applications called RiskMon. The main idea of RiskMon is to use machine-learned ranking to assess risks. Although, users specifying security requirements for security tools is a challenging task, the framework design allows for user's expected behavior rather than developers practices. However, it is subjective since it relies on user's input of relevancy levels for permission groups (user's expectations) and their understanding of these permission groups for each trusted application. This may result in biased choices. Although this risk model provides a continuous and automated RA, it is considered as low (machine)-level and limited to Android Mobile Apps. Moreover, users rely on a diversity of platforms and operating systems which makes it challenging as it increases the knowledge burden on users in maintain security in these different devices [50].

Not limited to assessing information security risks, many studies in the literature advice that, aside from the "one-size-fits-all" approach, a targeted risk communication approach should be adopted where messages contain the required technical and non-technical context, engaging and above all examined to ensure if they have an impact on users or not [3][33][51][52][53][54]. Actually, when these messages are not understood by the user, this may result in negative consequences that experts blame users for. The authors of [54] suggest that to effectively communicate security risks, users should be categorized according to their IT knowledge. Whereas a user education approach in risk communication that improves user's self-confidence and stresses on his responsibility of his own protection is recommended by authors of [19][55][56]. However, [51] argue that due to the timing and used terminology, information security threats warnings are easily and often ignored. Hence, human security behavior is critical to ensure an efficient information security environment that does not depend on technology only. It is suggested that risk communication should go one step further to changing user's security behavior [57][58][59]. However, several studies have confirmed that users do not react in the same manner to the same security threat nor the same user make the same decision in all situations. Moreover, they stressed that due to different factors filtered through user's personality, intended behavior may differ from actual behavior [52][60][61][62]. Many studies have highlighted the influence of user's characteristics such as personality traits [63][64], demographics and mother tongue [65][66][67] and IT proficiency [68][69] on user's security behaviors. In addition to these characteristics, [70] identified other factors related to the used security software such as risk communication, usefulness and delivery methods. Further to that, [70] demonstrated the impact of user's characteristics from a holistic point of view on user's risk-taking behavior and why some users are at risk more than others. Their findings suggest that given a certain user behavior and different users, risk is not the same for all of them. This work will be based on their findings. These studies demonstrate the importance of a targeted user-focused and not fact-focused risk communication that transforms the user from being ill-informed to a security minded user.

III. User-Centric Information Security and Response (UCRAR) Framework

Many types of data are stored on user's devices such as photos, contacts, documents and messages that are accessed by different applications. The terms software and application will be used interchangeably to refer to any piece of software installed on user's device. However, the unauthorized modification or disclosure of this data may result in a number of undesirable consequences on the CIA and privacy of such data. As each application has different impacts on data, which suggests that the risk level is changing within the application. Actually, different processes within an application have different impacts, thus, generating different risk levels for the same application. As a result, no single risk level could be assigned to an application. Not limited to that, but the way in which the user uses these processes may escalate or de-escalate these risk levels. For example, in a financial-based mobile application there are a range of functionalities and services that have different levels of risk associated to them. Services where there is no sharing of user's data as in reading products, services and offers have no impact on data, thus, from an application based behavioral perspective, risk is kept to a minimum. However, this risk level could escalate when combined with other non-app related behaviors such as connecting to a public Wi-Fi network or using a non-updated version of the application. Another example is the process of adding a photo in the Facebook application. On the one hand, adding a photo of The London Eye, for example, has a *low* risk level whether the user's account is public or private. Whereas adding the same photo with location data may have an impact on user's privacy, thus, escalating the risk level to *medium* in a private account and possibly *high* in a public account. On the other hand, for the same process of adding a photo but of the user's child, for example, in a private account has a *medium* risk level that escalates to *high* when the account is public. These examples serve to demonstrate that the risk level of user's behaviors within an application process could change when combined with other behaviors within the same application. Thus, arguably, assessing the risk level

based on user's behavior may result in a more realistic and accurate assessment. To the best of the researcher's knowledge, assessing and calculating risk for each user behavior of each process within an application and combining it with other behaviors simultaneously, and using user-centric factors, i.e. user's characteristics, such as demographics, online activity, personality traits and IT expertise as additional risk factors to create a user-centric risk profile has not been investigated yet. Moreover, combining this user-centric risk assessment with system-level risk assessment and smoothing it with community-based risk data to create an individualized risk profile is a novel approach to security risk assessment. Therefore, the necessity for a timely user-centric risk assessment and communication approach that adapts to user's characteristics and can be used across services and technologies becomes more apparent.

The proposed User-centric Risk Assessment and Response (UCRAR) framework is composed of two main components as in Fig.1. Namely, the Risk Assessment component and the Risk Communication component. As part of the novelty of this proposed framework, user-centric factors are utilized, among other factors, in both components. To accomplish this, the following processes are established:

A. Risk Assessment Component

In this component, user's behaviors are monitored, security risks are assessed on both system and user level and an individualized risk profile is created accordingly. The functionality of this component is accomplished by the following processes:

1) Good (expected) behavior: Among the requirements to assess each behavior independently is a clear description of a good user behavior. Thus, this knowledge base will include a set of descriptors that suggest what a good behavior should be in a certain aspect and used as a reference for user security compliance. In password hygiene, for instance, a list of good behaviors related to password's behaviors will be provided such as the same password is not used for multiple accounts, frequency of changing passwords and not allowing web browsers/software/apps to store passwords.

2) Software detector: There are millions of software products in the world. For example, the number of applications in Google Play store increased from 400,000 in 2011 to 3.5 million in 2017 with an average of almost 6000 applications released on a daily basis [2]. However this fails to consider the existence of organizational applications. Many applications could be installed on the user's device. To individually risk assess each installed application would be a time consuming task. Thus, the aim of this process is to detect all installed software on user's device and assign a quantitative score to each detected software/app. This score could be determined in many ways such as level of application/service usage, how important the software is to the user or in terms of its CIA impact. To support the user and reduce the burden on him in individually scoring each installed application, especially if the number of installed applications is numerous, that may result in him dumping/rejecting the Risk Assessment tool, the categorization approach proposed by [49] is adopted. In this approach, applications are classified into groups according to their type/usage. Then, each group is assigned a certain score. This score assignment will be part of system startup/configuration where each group will be assigned a quantitative value by the user according to its importance from his perspective. A scale of 0-**very low** to 4-**very high** will be used. Then, each detected installed application will be mapped into its corresponding group and assigned a score accordingly resulting in an *app-score*. For example, applications are classified but not limited to as in Table 1. As a vulnerable/out-of-date application and those originating from an illegitimate source are possible sources of risk, application version, *app-ver*, and the name of the source/market from which the application was installed from, *install-name,* are detected.

Thus, the output of this process is the following tuple:

Sw-info = (*sw-id*, *app-score*, *install-name*)

where: *sw-id* is the software/app ID in Common Product Enumeration CPE.

3) User behavior monitor: With this continuously evolving threat landscape and the wide range of computing platforms and services accessed, the need to continuously monitor and assess user's behaviors in a timely manner becomes more apparent. Certain users' characteristics, i.e user-centric factors, were related to changing/influencing his risk level, as discussed in Section 2, suggesting that user's-centric factors need to be gathered. Hence, the functionality of this process is a two-fold:

- To continuously monitor user's behavior independently of the used software and compare it against good/expected behavior. This is done in near real-time and is event triggered. For example, if a user is to close a browser/app, he will be reminded to sign off from online service before closing.
- To collect user info in terms of the specified user's characteristics, i.e. user-centric factors. This data collection is done in three ways, namely, explicitly, implicitly and by taking a specialized test as in Table 2. For IT proficiency and service usage level user-centric factors, the worst-case scenario is adopted. Thus, the categories whom found to be in highest risk as of [70] are assumed as default values, i.e. non-IT professional and high service usage. As the user is using the system, his behavior is monitored and these categories will be adjusted according to a predefined set of metrics.

Thus, the output of this process is the following tuple:

B-info = (B-expected, B-actual, U-info),

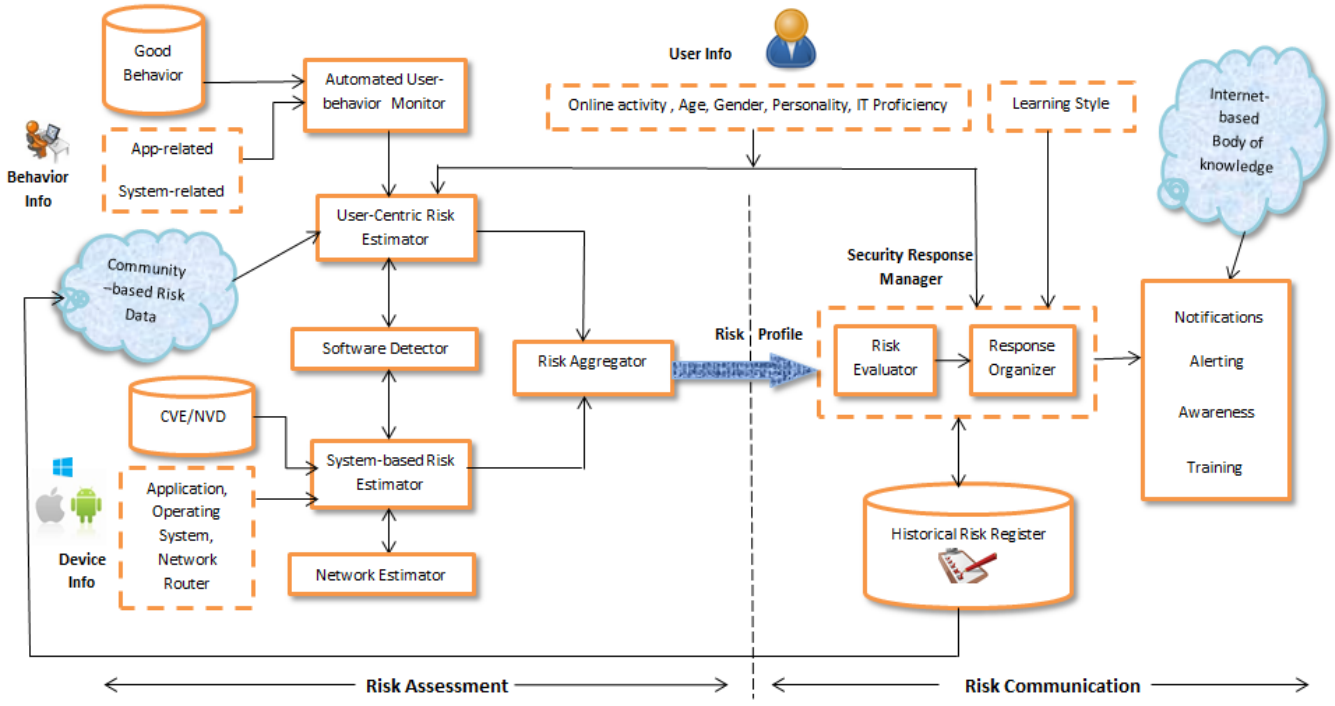

Fig. 1. The User-centric Risk Assessment and Response, UCRAR, Framework.

TABLE I. AN EXAMPLE OF SOFTWARE GROUPS

Social networking	e-banking
Messaging	Maps and navigation
News	Shopping
e-mail	Web access
Entertainment (games, music …etc)	Photography
Office applications (Ms Word, Ms Excel …etc)	Security
Operating system	

where B-expected is the expected good behavior derived from the Good Behavior knowledge base, B-actual is user's current behavior and U-info is user-centric factors expressed as the tuple (Age, Gender, Personality, Learning-style, IT-level, Use-level)

Nevertheless, due to this continuous monitoring, a very important aspect is that users need to trust this system and that it will not violate their privacy. They need to be aware that this monitoring is done for their own protection and any collected data will not be used for purposes other than those intended for risk assessment and will not be shared with any other application. This could be done by having the user, when installed the application, accept an agreement terms.

4) Community-based risk data: The proposed UCRAR is based upon user's behaviors in a certain point of time. Once the proposed system is running with many people using it, there is the chance to look at their user-centric factors, behaviors and responses in real time on a continuous basis. Information about users, behaviors and responses are fed into this Community-Based Risk Data in an anonymized form on a continuous basis. Hence, those found statistically significant correlations according to [70] could be re-evaluated and the user-centric risk estimation will be modified accordingly. For example, if the user-centric factor of age no longer has a statistically significant correlation with a certain behavior or a new user-centric factor becomes significant for a behavior then the system will adapt accordingly. The system has all required information to do this so called re-evaluation by mapping user's actual responses to a more meaningful risky/non-risky decision. This will allow it to move beyond the static point in time to a continuous understanding of these factors and correlations. Therefore, by knowing the actual behavior and response, those found significant correlations will be truly significant. Further to that, new threats might be introduced and impact a behavior quite differently depending on user-centric factors. As such, those relations are periodically revised such as every six months. Not limited to that, user's responses will be periodically used to intelligently re-measure user-centric factors. For example, user's IT-level could be changed from a non-IT professional to an IT-professional based on his behavior. These examples serve to demonstrate that UCRAR can dynamically adapt to changes in user-centric factors. Hopefully, this process will be used as feedback mechanism to keep the system up-to-date and gradually move away from behavioral intent to actual behavior.

TABLE II. SETTINGS OF USER-CENTRIC FACTORS

User-centric factor	Description	Determined
Age	Users will be classified into three age groups: 18-30 years, 31-50 years and 51+ years	Offline. By explicitly answering a direct question, as part of system setup/configurations
Gender	Users will be classified as either male or female	
Personality	According to their BFI score users will be classified as either high or low in one of the personality traits of Openness, Conscientiousness, Extraversion, Agreeableness and Neuroticism.	Offline. By using a BFI tool, as part of system setup/configurations
Learning style	According to their preferred learning style, users will be classified according to their VARK learning style as either Visual, Aural, Read/write or Kinesthetic	Offline. By using a LS tool, as part of system setup/configurations
IT level	According to predefined metrics to measure their IT expertise such as settings and modification of web browser configurations, frequent use of shortcut keys and the use of advanced features in software/apps such as section breaks and cross sections in MS Word and macros in MS Excel, the user will be assigned an IT proficiency level of either professional or not	Online. Determined implicitly by the User Behavior Monitor
Service usage	According to predefined metrics to measure their service usage and online activity such as number of unique IP addresses accessed, number of hours spent online on a predefined basis and volume of transferred data, the user will be assigned a service usage level of high usage, medium usage or low usage.	

5) User-centric risk estimator: This process performs a mapping of user behavior to applications. Hence, what is the user doing against what application given that a threat against an application maybe increased by a user's *insecure* behavior. User-centric factors will be considered as a risk factor when assessing risk on the user level. As the threat against a certain application maybe increased due to user's insecure behavior, behaviors are assessed, resulting in a risk score/level, *behavior-score*, and used as a risk factor. Additionally, other risk factors that are behavior-related are considered such as the application importance, *app-score*, as detected by the Software Detector process and the used communication channel. Consequently, assessing these user-centric and behavior-related risk factors will result in an individualized risk score/level, *behavior-risk* which is the output of this process.

6) Network estimator: Given that a vulnerable router is more likely to be exposed and used as a threat source [32], this process will monitor the status of the network in which the user is connected to and is kept to a minimum level. Hence, information about the used network devices, i.e. routers, are collected and passed to the System-Based Risk Estimator. Router information will be expressed in terms of router's software name and version and passed to System-Based Risk Estimator to check it for vulnerabilities. Thus, the output of this process is the parameter *r-id* which is the ID of the software executed on the router in CPE.

7) System-based risk estimator: As perfect security is considered to be unachievable for information systems, then the goal is to achieve a security level that is deemed appropriate to user's needs and requirements. A vulnerable software could be exploited by attackers compromising the system where this software is running [6] such that the more vulnerabilities in a software the less secure it is and, eventually, the lower its trustworthiness level. This process analyses and calculates security risks on system level. This is accomplished by checking all installed applications, router software and also platform information in terms of the used Operating System for vulnerabilities. For each of the previously mentioned, the System-Based Risk Estimator will check vulnerabilities knowledge bases such as NVD and CVE for known vulnerabilities and calculate a software risk score accordingly. Then, a final system risk score, *system-risk*, will be calculated which is the output of this process.

8) Risk aggregator: The purpose of this process is to evaluate/assess security risks based on information obtained from User-Centric Risk Estimator and System-Based Risk Estimator and generate a risk profile that adapts to users accordingly. Hence, this risk profile is composed of a set of parameters that are required by the Security Response Manager to do its job. This Aggregator will assess and analyze the security risk and determine the final risk score, *overall-risk*. However, the quality of the risk assessment depends on the accuracy and granularity of data provided by the previously mentioned processes. Thus, the output of this process is the generated risk profile as follows:

Risk-Profile=(*B-actual, U-info ,overall-risk ,risk-level, date*)

where *overall-risk* is the quantitatively expressed and calculated overall risk score, *risk-level* is the qualitatively expressed overall risk level and *date* is the date and time stamp this behavior was performed.

The operational flow in this Risk Assessment Component is as demonstrated in Fig 2.

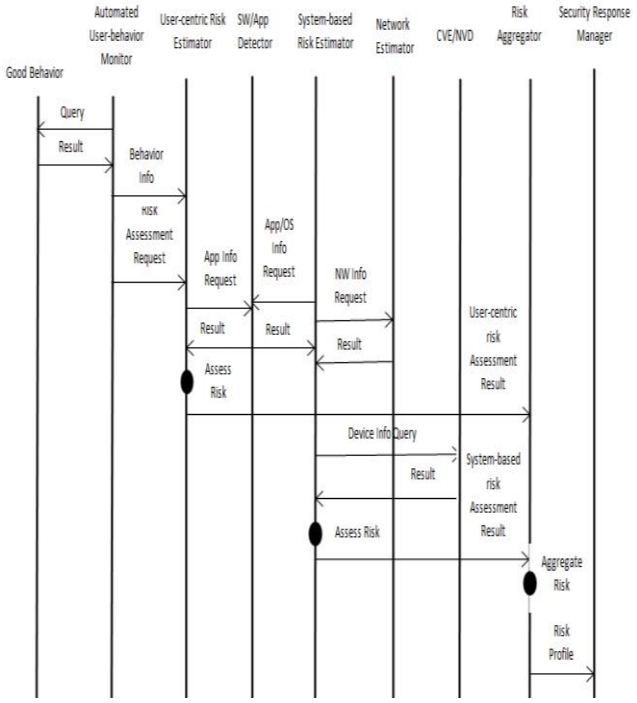

Fig. 2. Operational Flow in the Risk Assessment Component of UCRAR

B. Risk Estimation Models

As UCRAR provided a mechanism for understanding both system and user/behavior based risk and how to respond to them, a mechanism for estimating such risks is required. For the purposes of this Paper, three risk estimation models are proposed. These are a System-based, User-centric and Aggregated Risk Estimation Models to be used by the System-based Risk Estimator, User-centric Risk Estimator and the Risk Aggregator processes of UCRAR's Risk Assessment Component.

1) System-based risk estimation model: For the system-based risk estimation, a vulnerability-oriented approach will be used to assess and analyze security risks on the system level through the use of CVSS scoring algorithm [37]. Accordingly, any estimated risk score/level in UCRAR will be in accordance with the used CVSS scoring system, i.e. 0..3.9 low risk, 4..6.9 medium risk and 7..10 high risk. The nature of the proposed model allows the use of any software risk scoring methodology utilizing a CVSS scoring algorithm. Thus, the methodology proposed by [21] will be used to calculate the risk score of installed applications, *app-risk*, the used Operating System, *os-risk*, and router's software, *nw-risk*. Additionally, the source name of the installed application, *install-name*, is used as a risk factor. Since this risk factor is application-specific, it will be added to the calculated *app-risk*. If the application was installed from an illegitimate source, then the final security score of the application, *app-risk*, is calculated as follows:

IF *install-name* = illegitimate THEN (1)

{increase app risk level from low to medium}

IF 0<= *app-risk* <= 3.9 THEN *app-risk* = 4

{increase app risk level from medium to high}

ELSE IF 4<= app-risk <=6.9 THEN app-risk = 7

Therefore, the final system risk score, *system-risk*, is calculated as follows:

$$System\text{-}risk = app\_risk * w_{app} + os\_risk * w_{os} + nw\_risk * w_{nw} / (w_{app}+w_{os}+w_{nw}) \quad (2)$$

where w_{app}, w_{os} and w_{nw} are subjective weights.

Unfortunately, there is no evidence yet on how to weight *app-risk*, *os-risk* and *nw-risk* or suggest the proportion of impact each of them has on the system risk score/level, *system-risk*. Thus, these weights are suggested as 0.5, 0.3 and 0.2 respectively. However, the proposed model allows for a variety of ways such that whenever future research is available regarding this proportion, the proposed model could easily adopt to it.

2) User-Centric risk estimation model: Assessing user-centric and behavior-related risk factors will result in an individualized risk score/level, *behavior-risk*. In order to understand what needs to be measured and quantified , a list of possible user's behaviors is necessary. Nevertheless, it is unrealistic to assume all possible user's behaviors especially with the existence of multiple platforms and the increasing number of applications on a yearly basis [2]. Therefore, structuring it will provide a more meaningful risk assessment. Accordingly, a categorization of user's behaviors is suggested as in Fig. 3. Namely, these behaviors could usefully be categorized as System/Device-related behaviors and application-related behaviors that are further categorized according to the nature of the behavior and type of data accessed. Data is categorized according to the risk and impact on user's CIA and privacy when this data is modified or disclosed.

a) Application-Related Behaviors

The impact of consequences (CIA and P) of various user behaviors generate different risk levels within an application as discussed in section 3. Not limited to assessing user's behaviors, but behavior-related risk factors are assessed such as the used password, the used communication medium and account type if any. Among the several risk methodologies discussed in section II is CRAMM [26]. Seven impact consequences adopted from CRAMM are identified. Namely, impacts of disruption (D), personal privacy (P), data corruption (DC), embarrassment (E), financial lost (F), legal liability (LL), personal safety (S). As it is hard to assess this from one user to another due to different user-centric factors and to provide a fine-grained valuation that reduces the burden on the user in terms of user input, the potential consequences will be assessed and assigned for each behavior category. Then, each behavior will be mapped into its corresponding category. An example of potential consequences is as in Table 3 where they are rated as 0-Low, 1-Medium and 2-High.

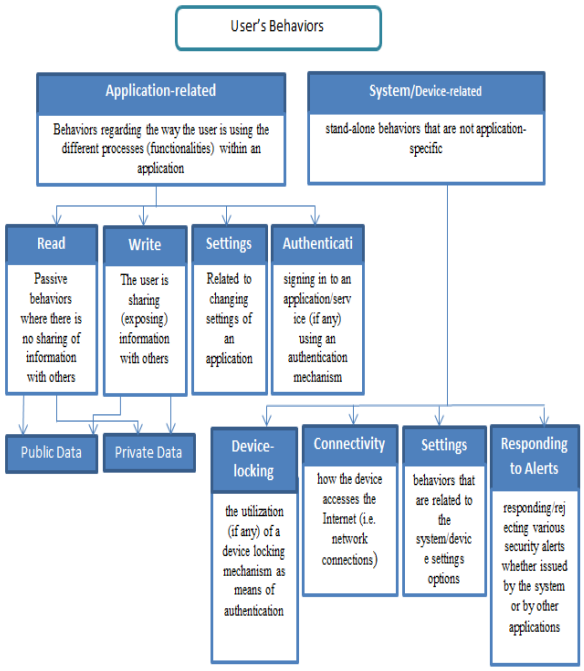

Fig. 3. A Suggested Categorization of User's Behaviors.

TABLE III. AN EXAMPLE OF SUGGESTED BEHAVIOR CONSEQUENCES

	Suggested Consequences						
Behavior Category	E	F	P	DC	LL	S	D
Read-private-data	**2 (H)**	**0 (L)**	**2 (H)**	**2 (H)**	**0 (L)**	**0 (L)**	**1 (M)**
Write-private-data	**1 (M)**	**2 (H)**	**2 (H)**	**2 (H)**	**1 (M)**	**0 (L)**	**0 (L)**
Write-public-data	**1 (M)**	**0 (L)**	**1 (M)**	**1 (M)**	**0 (L)**	**0 (L)**	**1 (M)**

To estimates risk, a matrix-based approach will be used and a risk matrix is generated for each consequence as in Matrix 1.The first step in assessing the behavioral risk score, *behavior-score*, is by mapping the behavior's potential consequences and the application's importance level *app-score* as detected by the Software Detector process in Matrix 1. This will result in seven quantitative scores (one for each consequence). Second, based on the "worst case scenario" principle [45], the maximum value resulting from the Matrix 1 is used. Hence, a behavioral risk score, *behavior-score*, will be generated as:

$$behavior\text{-}score = \text{MAX}(consequences) \quad (3)$$

		Consequence/ Attribute / Connectivity		
		Low	Medium	High
app-score	0	0	1	2
	1	1	2	3
	2	2	3	4
	3	3	4	5
	4	4	5	6

Matrix 1: UCRAR Risk Matrix

The same approach is used for estimating behavioral-related factors such as the used password *auth-score* and the used communication channel *connect-score* if any. For calculating auth-*score*, password's hygiene is checked for several attributes such as its length and password reuse. An authentication risk matrix is generated for each attribute as in Matrix 1. Each password attribute is assessed as 0-Low, 1-Medium or 2-High. After mapping the application's importance level *app-score* and password's attributes in Matrix 1, the maximum value resulting from the above risk matrix is used. Whereas for estimating *connect-score*, a risk level is pre-assigned for each type of communication channel such as Low for 3G/4G, Medium for Bluetooth, NFC and private WiFi and High for Public WiFi. These risk levels are based on the security measures utilized for data transmission by the communication channel. The used communication channel's pre-assigned risk level is mapped with the related *app-score* in Matrix 1 to generate a *connect-score*. Hence, the resulting *behavior-score/auth-score/connect-score* is a quantitative value from 0 to 6. However, based on findings of [70], two situations are identified. If the assessed behavior is significantly correlated with a user-centric factor, then the resulting *behavior-score* is recalculated first based on the significance correlation risk factor as explained in the next section. then *behavior-risk* is calculated as in (4). Otherwise, *behavior-risk* is calculated as in (4). In both cases, the resulting *behavior-risk* will be normalized because all scores used in the risks calculations are from 0 to 10.

Given that the disclosure or modification of private data in a private Facebook account, for example, has a lower risk level than in a public account, a pre-set score of 1 and 2 is assigned for private and public accounts respectively as the *account-type-score* (if any).

Finally, to estimate *behavior-risk*,

$$behavior\text{-}risk = \text{AVG}(behavior\text{-}score, auth\text{-}score, connect\text{-}score) + account\text{-}type\text{-}score \quad (4)$$

b) System/Device-Related Behaviors

A risk estimation model is proposed for each system/device-related behavior category. Connectivity behaviors are assessed in the same approach as in estimating *connect-score*. In responding to alerts or settings behaviors, risk is estimated for these behaviors as stand-alone behaviors regardless of application importance, *app-score*. If an alert is ignored/no action taken by the user or a setting is disabled, then risk is high and an averaging approach is used to calculate *behavior-score* by adding the values at both ends of the level's scale (high risk level has a risk score between 7 and 10) and dividing it by 2 as in (5). For Device locking behaviors, risk is not only estimated if such control is utilized or not, but also the degree it complies to good authentication behavior such as password hygiene. Hence, risk is estimated such that If no lock is used, then risk is high and *behavior-score* is estimated as in (5). If device lock (PIN) is used, then it is assessed for its hygiene using Matrix 1 in an approach similar to that of estimating *auth-score*.

$$behavior\text{-}score = (7 + 10)/2 = 8.5 \quad (5)$$

The resulting *behavior-score* is recalculated based on the significance correlation risk factor (if any) resulting in *behavior-risk*.

3) The significance correlation risk factor: The novelty of this risk assessment scheme is that a different risk profile is created for the same behavior given a number of users. Based on our work [70], it was found that the risk score/level of a behavior may be positively or negatively affected by certain user-centric factor such as personality trait, age and IT expertise. Thus, the significance of the correlation between a user's behavior and user's-centric factors (if any) is used as a risk factor to reassess the behavioral risk score, *behavior-score*. However, when considering the significance correlated risk factor, two situations are identified, namely, the significance correlation risk factor for application-related behaviors and the significance correlation risk factor for system/device-related behaviors. In the former, the significance of a correlation implies that due to certain user-centric factors values (Low, Medium, High), the likelihood of a security threat is either decreased or increased. Asset value is equivalent to the application's importance level from the user's perspective whereas how easy a security breach may occur depends on the type of user's behavior. Hence, the significance correlation matrix, matrix 2, is adopted from [10] where user-centric factor value, *behavior-score* and *app-score* are used instead of threat likelihood, ease of exploitation and asset value respectively in the original matrix.

User-centric factor Value		**Low**			**Medium**			**High**		
behavior-score		**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
App-score	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Matrix 2: Significance Correlation Matrix

The proposed methodology for the significance correlation risk factor for system/device-related behaviors and application-related behaviors is as described in Figs. 4 and 5.

4) Aggregated risk estimation model: The proposed model for aggregating the user-centric risk score, *behavior-risk*, and the system-based risk score, *system-risk*, for application-related behaviors is as follows:

$$Overall\text{-}risk = (behavior\text{-}risk * w_{br}) + (system\text{-}risk * w_{sr}) \quad (10)$$

GET user-centric factor value, app-score, behavior-score.
IF behavior-score € {0,1,2} THEN low risk
ELSE IF behavior-score = 3 THEN medium risk
ELSE IF behavior-score € {4,5,6} THEN high risk
IF –ve correlation THEN (6)
IF user-centric factor = high THEN {decrease the risk }
user-centric factor = low level
MAP user-centric factor value, *behavior-score* and *app-score* in Matrix 2
GET new *behavior-score*
ELSE IF user-centric factor = low THEN {increase the risk }
user-centric factor = high level
MAP user-centric factor value, *behavior-score* and *app-score* in Matrix 2
GET new *behavior-score*
ELSE IF user-centric factor = medium THEN
user-centric factor = medium level
MAP user-centric factor value, *behavior-score* and *app-score* in Matrix 2
GET new *behavior-score*
IF +ve correlation THEN (7)
IF user-centric factor = high THEN {increase the risk}
user-centric factor = high
MAP user-centric value, *behavior-score* and *app-score* in Matrix 2
GET new *behavior-score*.
ELSE IF user-centric factor = low THEN {decrease the risk }
user-centric factor = low
MAP user-centric factor, *behavior-score* and *app-score* in Matrix 2
GET new *behavior-score*.
ELSE IF user-centric factor = medium THEN
user-centric factor = medium
MAP user-centric factor, *behavior-score* and *app-score* in Matrix 2
GET new *behavior-score*.

Fig. 4. Application-Related Behavior's Methodology for Significance Correlation Factor.

GET user-centric factor value, *behavior-score*.
IF –ve correlation THEN (8)
IF user-centric factor = high THEN {decrease the risk }
behavior-score = *behavior-score* - 1
ELSE IF user-centric factor = low THEN {increase the risk }
behavior-score = *behavior-score* + 1
ELSE IF user-centric factor = medium THEN
Neither increase nor decrease the risk score.
IF +ve correlation THEN (9)
IF user-centric factor = high THEN {increase the risk }
behavior-score = *behavior-score* +1
ELSE IF user-centric factor = low THEN {decrease the risk score}
behavior-score = *behavior-score* - 1
ELSE IF user-centric factor = medium THEN
Neither increase nor decrease the risk score

Fig. 5. System/Device-Related Behavior's Methodology for Significance Correlation Factor.

Where w_{br} and w_{sr} are subjective weights and suggested as 0.5. Unfortunately, there is no evidence yet on how to weight *behavior-risk* and *system-risk* or suggest the proportion of impact each of them have on the final risk score/level, *overall-risk*. However, the proposed model allows for a variety of ways such that whenever future research is available regarding this proportion, the proposed model could easily adopt to it.

As a vulnerable application is not considered, arguably, as a threat source when assessing risks of system/device-related behaviors such as in not utilizing a device lock or in connecting to a public WiFi network. Moreover, the threat is in the behavior itself as a stand-alone behavior regardless of compound risks. Thus, *overall-risk* for system/device related behaviors is the same as the user-centric risk score as

Overall-risk = behavior-risk (11)

C. Risk Communication Component

The second component of the framework, Risk Communication, starts by receiving the individualized risk profile form the Risk Aggregator, analyzing it and deciding on the most suitable form of communicating/educating the risk to the user. Different from the related work described in Section II, the proposed model is intended to assess and communicate risks in near real time and alert the user before taking further action. Evidence suggests that static risk communication may result in users becoming inattentive to messages delivered [51][71][72]. Hence, the robustness of risk communication should be suited to the encountered risk by providing the user with real time needed security education about his risk taking behavior. This is done in an individualized persuasive manner to transform him from being ill-informed to a security minded user. To accomplish this risk communication, the following processes are established:

1) The security response manager: Based on the user's behavior risk level, the Security Response Manager will make a decision on what the next step is. However, when communicating risk to the user, the response manager will decide upon the best form of persuasive technology that best suits the user based upon *U-info* that is part of the risk profile. Thus, to educate user's about security risks and promote good behavior, user-tailored messages that take into account the individual user-centric factors are used. Two sub-processes carry on the functionality of The Security Response Manager as follows:

- **Risk Evaluator**: Once the risk profile is received, the risk level is checked first. If the behavior is secure, i.e. low risk, then behavior-response-information is sent immediately to the Historical Risk Register. If the behavior is insecure, i.e. risk level is medium or high, then the risk profile is forwarded to The Response Organizer.
- **Response Organizer**: Prior to issuing a message, it will check the Historical Risk Register of previous incidents of the same behavior and the issued security messages related to it. Hence, the response mechanism of this process depends on two concepts, namely, informing the user of his behavior's risk score/ level and deciding on the best way to communicate/educate the user about his risk-taking behavior. Hence, based on the information received in the risk profile and historical data about the same behavior (if any) from the Historical Risk Register process, a gradual, individualized and persuasive response mechanism of varying gradual response levels is suggested.

2) Historical risk register: All user's behaviors, whether secure or insecure, and information related to it are continuously stored in this register/database for a limited time period then discarded. This time period will be reasonable enough to capture the latest changes in user's behavior without exhausting resources in storing too much data. Whenever a risk profile is received, it is compared with relevant historical risk data. The result of this comparison is used to determine the type/level of response. This will be stored as the following tuple:

res-behavior = (*b-actual, date, response, module, u- action, risk-score, risk level*) (12)

Where: *response* is the response level. However, 0 is used to indicate no response issued, i.e. secure behavior. *Module* is to indicate the type of recommended security education module (if any) of either security **aw**areness, **tr**aining or **no**ne, *Module* Є {aw, tr, no}. *u-action* is user's behavior towards a given module if any, i.e. **i**gnored, **p**ostponed or **o**beyed *U-action* Є {i,p,o} Additionally, this information will be used by the Security Response Manager when issuing a motivation alert, user's behavior report and to identify areas in which the user has mostly behaved insecurely and in need of further education.

3) Alerts, reminders/notifications, awareness and training: Security is "rarely the user's primary goal" and users only try to protect themselves from risks salient to them [71]. This targeted risk communication goes beyond passively notifying/warning users of security risks to act as a tool to educating and training the user on good behavior to make security informed decisions whilst displaying the security message. This is accomplished through additional teaching/education in the user's preferred learning style such as gamification, video or podcast.

4) Internet-based Body of Knowledge: To educate the user about security, a form of targeted security education will be provided based on user's behavior focusing, mainly, on educating him of his risk taking behavior. This will be decided upon by searching an Internet based body of knowledge that is developed by a third party, or simply the Internet as a huge knowledge base for security information such that the required security information will be searched for, identified and located on the Internet. As the accuracy and effectiveness of such provided info should be evaluated, the creation of such knowledge base and evaluation of retrieved security information are outside the scope of work of this research and could be part of future work. Hence, operational flow in this component is as demonstrated in Fig. 6.

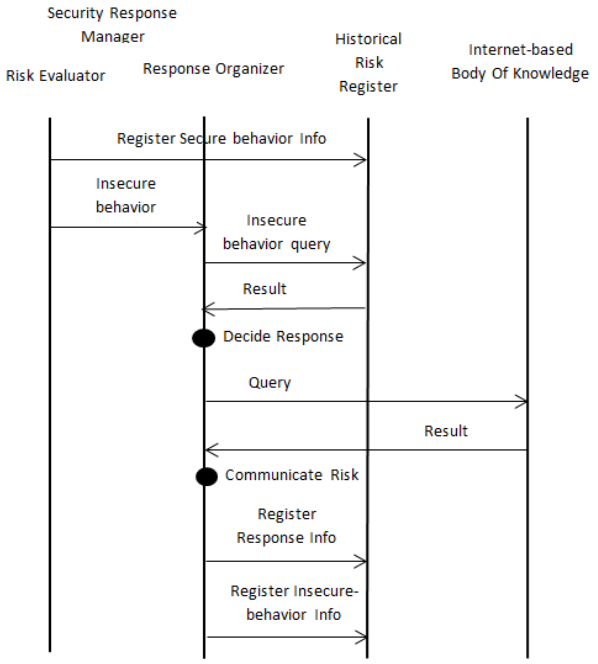

Fig. 6. Operational Flow in the Risk Communication Component of UCRAR.

IV. Evaluation of UCRAR

The resulting risk scores/levels from the Risk Assessment component will enable other processes of the proposed UCRAR, the Security Response Manager for example, to take that information and act accordingly. Given the aim and objectives of this paper to develop a user-centric approach towards risk assessment, a decision was made by the authors to focus on the Risk Assessment component of UCRAR and to have further work in the Risk Communication component as future work.

As UCRAR is dependent upon a variety of factors, whether user-centric such as IT proficiency and personality traits, or behavioral-related such as the used communication medium and authentication hygiene, the aim is to evaluate its effectiveness, feasibility and nature, i.e. how it works given a number of different users with different characteristics and behaviors. Furthermore, to empirically investigate whether the dynamics of the proposed UCRAR operate in the envisaged manner and the factors identified to impact risk do have an impact upon the resulting risk scores/levels. However, to evaluate the model, there exists a number of challenges in implementing the proposed model on real users and within a real environment. The need to develop the required controls to do the process of user monitoring and the development of several knowledge bases such as the community-based risk data are examples of such challenges. Although different approaches could be taken to evaluate the model, the most complete and comprehensive approach that will enable a comprehensive analysis of the model appeared to be a simulation-based approach. In this approach, a number of users with different risk profiles across the spectrum will be replicated. Hence, risk will be estimated/calculated independently for each user.

In order to do a walkthrough of the proposed model and understand, in a categorized fashion, how different users are impacted by risk, a scenario-based simulation based upon a variety of users' profiles from one end to the other is designed considering the following:

1) All possible user-centric factors permutations for different users.

2) To understand the nature of how user's behaviors impact the risk scores/levels, behaviors included in the scenario reflects examples of each behavior type from the proposed Categorization of Behaviors as in Fig. 3 .

3) Behaviors selected demonstrate the difference between the resulting risk scores/levels of behaviors that were found to be most significantly correlated with a certain user-centric factor and those that were not (Behavior 6).

4) Varying *app-scores* with low, medium, high and very high importance are assumed.

The simulation is done as follows:

- The scenario is assumed to model the nature of the risk process. However, it is worth highlighting that the scenario selected is an example and has no specific basis only that it introduces a number of different risks a typical user might encounter.
- A variety of users with different user-centric factors are assumed.
- The model is applied and risk is calculated.
- Results are analyzed to understand how different users are impacted by risk

Hence, assuming the scenario of a user is sitting in Starbucks coffee shop and connected to their WiFi. While browsing his email's inbox, he opened an email from an unknown sender asking for his credentials and bank account number to claim a won lottery prize, but ignored it. Then, he opened another email from a friend and downloaded a greeting card that was attached to it. Meanwhile, he was alerted that a new update for his AntiVirus application is available, but cancelled it. At that time, a friend came to sit with him where they chatted for an hour. When his friend left, he unlocked his device and started browsing job websites. When a job request was found and wanted to apply for it, he was asked to register with a username and password first. After registration, he was prompted by the browser to remember this password and accepted. Subsequent to signing in, he was redirected to another website unknown to him to download and fill an application form. Ignoring an alert not to open this document, he opened the document, filled it up and clicked on "SEND". As he was typing the BBC News website's URL, he was alerted that a preinstalled application (AntiVirus application) is slowing down his device so he immediately disabled it and continued browsing. Starbucks's Router is using CISCO AIRONET access point software version 8.1 (112.3). The user is using a Samsung Galaxy Note 3 running Android version 4.4.4, Google Chrome application version 39.0.2171.45 and Email application version 4.2.2.0200. The user is using Symantec Mobile Security as an

AntiVirus application. All installed applications were downloaded from GooglePlay. Both the email's password and the job website's password comply to all password hygiene attributes except that the former does not contain uppercase letters and the same password is used for his Twitter account while the latter is 5 characters long. The used device pin lock is 1111. The user rated the importance of Twitter application as low (*app-score* = 1), Chrome as medium (*app-score* = 2), Email as High (*app-score* = 3) and Symantec Mobile Security as very high (*app-score* = 4). However, all applications were installed from Google Play which is a legitimate market.

The types of users assumed along with their user-centric factors are as in Table 4. Given the above scenario, a list of insecure security behaviors, i.e risks, along with their behavior type and the user-centric factor that was found to have the most significant correlation with that behavior according to findings of [70] are as in Table 5.

To assess risk of the behaviors mentioned in Table 5, risk is estimated on the system level first then on the user level.

To estimate risks on the system level, *system risk* :

Using the methodology proposed by [21], the security scores of each of the mentioned applications , *app-risk*, the used Operating System, *os-risk*, and router's software, *nw-risk*, are calculated. Then, *System-risk* is estimated for the applications of Chrome, Email and Mobile security as 5.8, 5.8 and 5.5 respectively.

To estimate risks on the user level, *behavior- risk* and *overall-risk*:

For each behavior in Table 5, risk of the behavior, *behavior-risk*, is estimated first followed by estimation of aggregated/final risk, *overall-risk* resulting in scores as in Table 6. This is done according to user's rating of used applications, Twitter's *app-score* = 1, Chrome's *app-score* = 2, Email's *app-score* = 3 and Symantec Mobile Security's *app-score* = 4. For space limitations detailed calculations are not included. These are available upon request.

TABLE IV. USER"R-CENTRIC FACTORS --- * USER WITH HIGHEST RISK PROFILE, ** USER WITH LOWEST RISK PROFILE

User	Personality Traits					Age	Gender	IT Proficiency	Service Usage
	Extra.	Agree.	Con.	Neuro.	Open.				
A	High	Low	Low	High	Low	40 Years	Male	IT Pro.	Low
B	High	High	High	Low	Low	55 Years	Female	Non IT Pro.	Medium
C	Low	Low	High	Low	High	27 Years	Male	IT Pro.	High
D*	High	Low	Low	High	Low	19 Years	Female	Non IT Pro.	High
E**	Low	High	High	Low	High	52 Years	Male	IT Pro.	Low

TABLE V. A LIST OF USER'S INSECURE BEHAVIORS

B#	Behavior	Behavior Type	Most Significant Characteristic	Correlation
B1	Connecting to a public WiFi	System-Device/ Connectivity	Service Usage	Positive
B2	Same password for multiple Accounts	Application/Authentication	IT proficiency	Negative
B3	Did not delete a suspicious email	Application/ Write - Private data	Age	Negative
B4	Opened an attachment in an email from a friend without checking	Application/ Read -Private data	IT proficiency	Negative
B5	AntiVirus software not updated	System-Device / Settings	IT proficiency	Negative
B6	Cancelled a security related update	System-Device / Responding to alerts	None	None
B7	Did not disable WiFi when not using it	System-Device / Connectivity	Gender	Negative
B8	Device Lock of "1111"	System-Device / Device locking	Con. Personality trait	Negative
B9	Allowed browser to remember his password	Application/ Write - Private data	Service usage	Positive
B10	Opened a document despite security warning	System-Device / Responding to alerts	Age	Negative
B11	Disabled AntiVirus software	Application/ Settings	Con. Personality trait	Negative
B12	Downloaded a file from an unknown website	Application/ Write - Public data	Con. Personality trait	Negative

TABLE VI. THE RESULTING USERS' RISK PROFILES

B#	Calculated risk	Users A	B	C	D*	E**
B1	•behavior-risk	7.5	8.5	9.5	9.5	7.5
	overall-risk	7.5	8.5	9.5	9.5	7.5
B2	▲behavior-risk	6.3	8.8	6.3	8.8	6.3
	overall-risk	5.9	7.2	5.9	7.2	5.9
B3	▲behavior-risk	6.3	6	6.7	6.7	6
	overall-risk	6.1	5.9	6.3	6.3	5.9
B4	▲behavior-risk	6	6.7	6	6.7	6
	overall-risk	5.9	6.3	5.9	6.3	5.9
B5	•behavior-risk	7.5	9.5	7.5	9.5	7.5
	overall-risk	7.5	9.5	7.5	9.5	7.5
B6	•behavior-risk	8.5	8.5	8.5	8.5	8.5
	overall-risk	8.5	8.5	8.5	8.5	8.5
B7	•behavior-risk	7.5	9.5	7.5	9.5	7.5
	overall-risk	7.5	9.5	7.5	9.5	7.5
B8	•behavior-risk	8	6	6	8	6
	overall-risk	8	6	6	8	6
B9	▲behavior-risk	5	5.3	5.7	5.7	5
	overall-risk	5.4	5.6	5.8	5.8	5.4
B10	•behavior-risk	8.5	7.5	9.5	9.5	7.5
	overall-risk	8.5	7.5	9.5	9.5	7.5
B11	▲behavior-risk	10	7.5	7.5	10	7.5
	overall-risk	7.8	6.5	6.5	7.8	6.5
B12	▲behavior-risk	5.3	4.7	4.7	5.3	4.7
	overall-risk	5.6	5.3	5.3	5.6	5.3

*user with highest risk profile , **user with lowest risk profile, ▲application-related behavior, ● system/device-related behavior

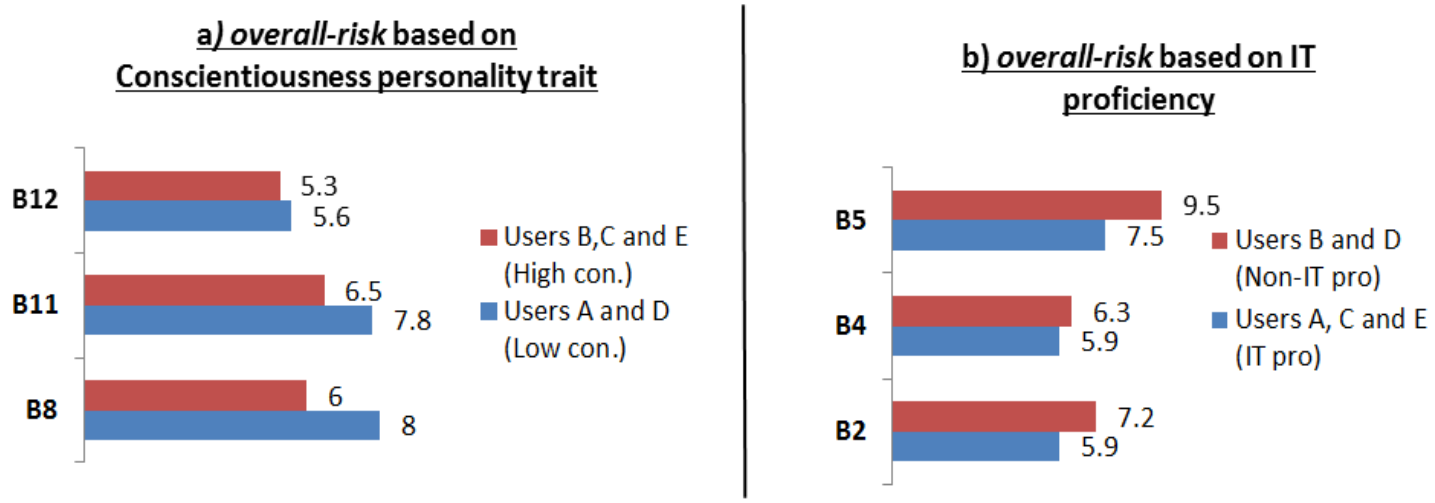

Fig. 7. Overall-Risk based on Personality, IT Proficiency.

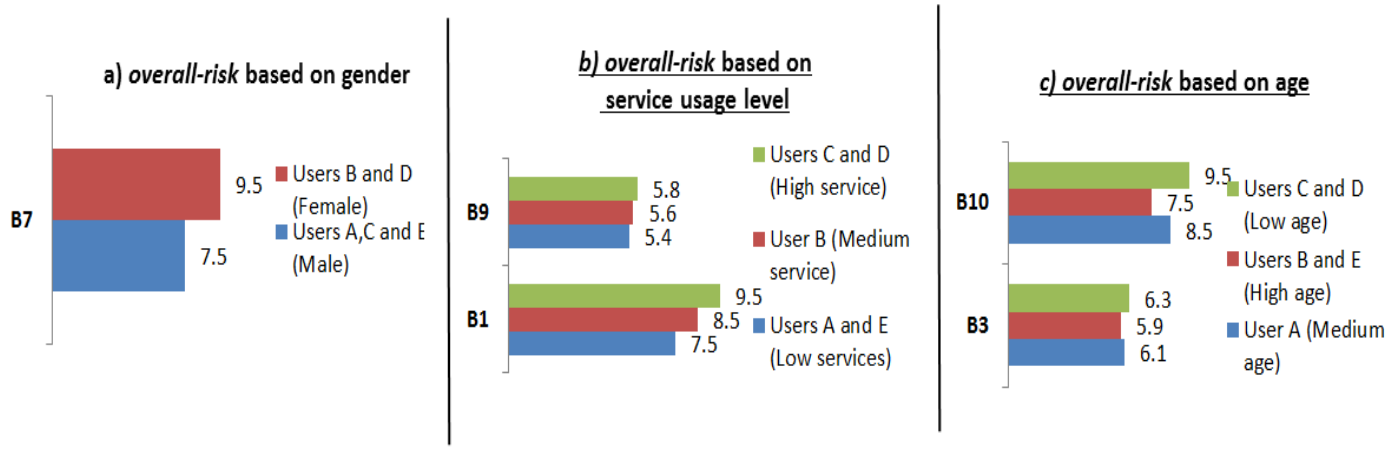

Fig. 8. Overall-Risk based on Gender, Service-usage Level and Age.

A comparison of these results based upon the impact of user-centric factors on the resulting risk scores/levels, highlights a number of trends. As IT proficiency and conscientiousness personality trait user-centric factors were found to be most significantly negatively correlated with behaviors B2, B4 and B5 for the former and behaviors B8, B10 and B12 for the latter, this impact is explicit. IT professionals and those with a high level of conscientiousness personality trait were in lower risk than non-IT professionals and users with lower levels of conscientiousness as in Fig. 7 a and b. A similar impact was apparent for males over females as gender user-centric factor is most significantly negatively correlated with behavior B7 as in Fig. 8 a. The user-centric factors of age and service usage levels are categorized in three levels of low, medium and high with an opposing significant correlation with behaviors B1 and B9 for the former and B3 and B10 for the latter. As illustrated in Fig. 8 b and c, the variations in these user-centric factors resulted in varying risk profiles for users as the higher the service usage level of the user the higher the risk and conversely, the older the user the lower his risk level. These results are in line with findings of [70].

Opposing to the above mentioned behaviors resulting risk scores/levels, behavior B6 that was found not to be significantly correlated with any of the studied user-centric factors resulted in a unified risk score/level, i.e. 8.5 High risk, for all users as in Fig. 9. The comparison between resulting risk scores/levels of other behaviors and those of behavior B6 serve to show how the proposed risk models take into account the variations in the most significant correlated user-centric factors when calculating risk. Moreover, it shows the difference between an individualized and a none-individualized resulting risk scores/levels. To this end, different risk profiles were obtained for the same behavior as a result of variations in users-centric factors. This suggests that the proposed model can adapt to these variations resulting in a more realistic and individualized risk score/level.

This simulation is based on a time line scenario of activities. To reflect the evolving nature of risk over time, Fig.10 illustrates how the risk score changes for each user as the time goes through the scenario based upon the behaviors being exhibited. As *system-risk* is almost constant of 5.8, the resulting deviation of risk scores from 5 to 10 is based upon a single scenario. However, in other scenarios with other systems, different varying system risks will be included which will result in varying risk scores across the spectrum, i.e from 0 to 10.

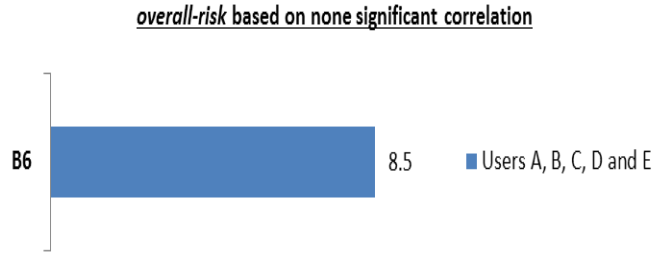

Fig. 9. Overall-Risk based on None Significant Correlation.

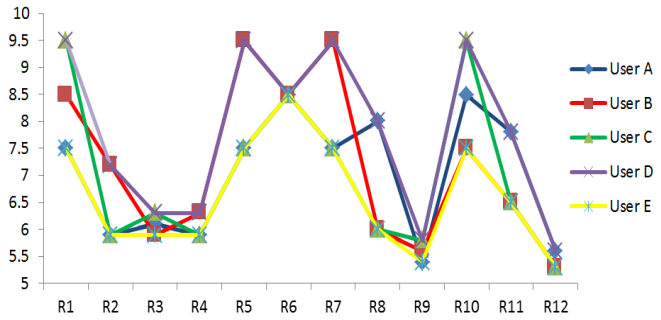

Fig. 10. Resulting Users' Risk Profiles Over Time.

To this end, the analysis of the simulation results provided an indication that risk could be assessed differently for the same behavior based upon a number of user-centric and behavioral-related factors resulting in an individualized granular risk score/level. This granular risk assessment, away from high, medium and low, provided a more insightful evaluation of both risk and response. The analysis of results was also useful in demonstrating how risk is not the same for all users and how the proposed model is effective in adapting to differences between users offering a novel approach to assessing information security risks.

V. Discussion

A user-centric risk assessment and response framework that takes into account, when estimating risk, variations in user's characteristics is proposed. In addition, other behavioral-related factors were considered in estimating risk resulting in a risk score/level not of a single behavior but of compound risk. Using a scenario-based simulation of a variety of users with different risk profiles, the proposed risk estimation models were applied and results analyzed. Actually, this was an opportunity to show that risk has to be based on the user and there are factors whether user-centric or behavioral-related that influences his behavior and risk score/level accordingly. This is evident as different risk profiles were obtained for the same behavior as a result of variations in users'-centric factors such as his age, personality trait and service level usage showing that the proposed model can adapt to change in these factors to produce an individualized risk score/level. However, when comparing the resulting risk scores/levels of a certain behavior for different users, as in B4 for instance, we are able to see no difference in the risk level, i.e. medium. From the user's perspective, this increase or decrease in the risk score but within the same risk level may not be relevant. Consequently, the nature of the proposed models do not allow for a decrease or an increase of 3, for instance, in one hit. Thus, this level of granularity is picked up and understood by the security response manager that this 0.5 increase or decrease, for example, does mean something and acts accordingly. This is similar in concept to the concept of "Fever" in the human body. As the normal temperature is 37.5^{O}c, an increase of temperature of 0.30^{O}c to 37.8^{O} implies that the person has high fever and a medical procedure has to be applied. Similarly, the temperature of 39^{O}c is still considered high fever but the difference is in how it is treated.

To this end, user-centric factors do contribute to the resulting risk scores/levels either by escalating or deescalating it. There is clear evidence to suggest that, in comparison to prior work, the proposed risk assessment methodology is a novel approach that incorporates user-centric and behavioral-related factors when calculating risk.

VI. Conclusion

A user-centric framework that assesses and calculates risk on both user and system level was proposed. This framework is composed of two components, risk assessment and risk communication. Three risk estimation models were proposed to calculate both *behavior-risk* and *overall-risk*. These models used a number of risk factors when estimating risk. The risk assessment component of the proposed framework was evaluated using a scenario-based simulation of different users and results analyzed. The proposed risk calculation models worked in the way they were expected to. The analysis of results revealed a number of trends and relations. Further to that, the analysis provided evidence that the level of impact and contribution of risk factors is not fixed for all users and behaviors. There are other sources of risk to the user other than his actual behavior. These sources range from user-centric to behavioral-related. Aside from the traditional "*one size fits all*" solution in prior literature, encouragingly, the results of this simulation provided an indication that risk could be assessed differently for the same behavior based on a number of user-centric and behavioral-related factors resulting in an individualized and timely risk score/level. Future work will focus on evaluating the risk communication component of UCRAR first, then have a running/implemented version of UCRAR to conduct a series of experiments with real users to evaluate its effectiveness as a whole.

References

[1] Number of Internet Users *(2017) - Internet Live Stats* (2017) [Online]. 2017. Available at: http://internetlivestats.com/internet-users

[2] Statista - *The Statistics Portal* (2017) [Online]. 2017. Available at: http://statista.com.

[3] Bawazir, M., Mahmud, M., Abdul Molok, N., Ibrahim, J. (2016) Persuasive Technology for Improving Information Security Awarenessand Behavior: Literature Review. In: (ICT4M) 6th International Conference on Information and Communication Technology for The Muslim World. 2016, IEEE, pp. 228-233

[4] Symantec, (2018) *Symantec Internet Security Threat Report*. Symantec Corporation.

[5] Symantec, (2017) *Symantec Internet Security Threat Report*. Symantec Corporation.

[6] Kaspersky, (2016) *Kaspersky security bulletin 2014*. Kaspersky Labs

[7] European Agency For Network and Information Security (ENISA), (nvd.) *Inventory of Risk Management- Risk Assessment Methods and Tools*. [Online]. Available at: http://rm-inv.enisa.europa.eu/methods.

[8] Tiganoaia, B. (2012) Comparative Study Regarding The Tools Used for Security Risk Management. *Revista Academiei Fortelor Terestre*, 17(3), pp. 319-325.

[9] National Institute of Standards and Technology NIST Special Publication 800-30, Revision 1, (2012) *Guide for Conducting Risk Assessment*.

[10] The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC), (2011) *ISO/IEC 27005:2011, Information Technology- Security Techniques- Information Security Risk Management*. Switzerland.

[11] Karabacak, B. and Sogukpinar, I. (2005) ISRAM: information security risk analysis method. *Computers & Security*, 24(2), pp. 147-159.

[12] Talib, S., Clarke, N., and Furnell, S. (2010) An Analysis of information security awareness within home and work environments. In: *International Conference on Availability, Reliability and Security*. 2010, IEEE, pp. 196 - 203.

[13] Kritzinger, E. and Von Solms, S. (2013) Home user security from thick security-oriented home users to thin security-oriented home users. In: *Science and Information Conference*. 2013, pp. 340 - 345.

[14] Rao, U. and Pati, B. (2012) Study of Internet security threats among home users. In: *Fourth International Conference on Computational Aspects of Social Networks*. 2012, IEEE, pp. 217 - 221.

[15] Mylonas, A., Kastania, A., and Gritzalis, D. (2013) Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, pp. 47-66

[16] Zabaa, Z., Furnell, S., and Dowland, P. (2011) End- user Perception and Usability of Information Security. In: *5th International Symposium on Human Aspects of Information Security and Assurance (HAISA)*. 2011, pp. 97-107.

[17] Komatsu, A., Takagi, D., and Takemura, T. (2013) Human aspects of information security. *Information Management & Computer Security*, 21(1), pp. 5-15

[18] Mensch, S. and Wilkie, L. (2011) Information Security Activities of College Students: An Exploratory Study. *Academy of Information and Management Sciences*, 14(2), pp. 91-116

[19] Furnell, S. and Clarke, N. (2012) Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), pp. 983-988.

[20] Hansch, N. and Benenson, Z. (2014) Specifying IT security awareness. In: *25th International Workshop on Database and Expert Systems Applications*. 2014, IEEE, pp. 326 – 330

[21] Wu, B. and Wang, A. (2011) EVMAT: An OVAL and NVD Based Enterprise Vulnerability Modeling and Assessment Tool. In: *Proceedings of the 49th Annual Southeast Regional Conference*. 2011, ACM, pp. 115-120.

[22] Van Cleef, A. (2010) A Risk Management Process for Consumers: The Next Step in Information Security. In: *2010 Workshop on New security Paradigms (NSPW)*. 2010, pp. 107-114.

[23] Jing, Y., Ahn, G., Zhao, Z., and Hu, H. (2014) RiskMon: Continuous and Automated Risk Assessment of Mobile Applications. In: *Proceedings of The 4th Conference on Data and Application Security and Privacy*. 2014, ACM, pp. 99-110.

[24] Paul, S. and Vignon-Davillier, R. (2014) Unifying traditional risk assessment approaches with attack trees. *Journal of Information Security and Applications*, 19(3), pp. 165-181

[25] Wangen, G. (2017) Information Security Risk Assessment: A Method Comparison. Computer, IEEE, 50 (4), pp. 52-61

[26] Yazar, Z. (2011) A Qualitative Risk Analysis and Management Tool-CRAMM. *SANS Institue Information security Reading Room*,

[27] CORAS, The CORAS Method (n.d.) [Online]. Available at: http://coras.sourceforge.net. (Accessed: 15 December 2014).

[28] OCTAVE Available at: octave

[29] Magerit, (2006) *Methodology for Information Systems Risk Analysis and Management: Book 1- The Method*. Madrid: Ministerio de Administracones Publicas.

[30] Mehari, (2007) Overview. *Club de la Securite de l'Information Francis (CLUSIF)*,

[31] Bhattacharjee, J., Sengputa, A., Mazumdar, C., and Barik, M. (2012) A two-phase Quantitative Methodology for Enterprise Information Security Risk Analysis. In: *CUBE*. 2012, ACM, pp. 809-815.

[32] Alsaleh, M. and Alshaer, E. (2014) Enterprise Risk Assessment Based on Compliance Reports and Vulnerability Scoring Systems. In: *Proceedings of the 2014 Workshop on Cyber Security Analytics, Intelligence and Automation (SafeConfig)*. 2014, pp. 25-28

[33] Takahashi, T., Emura, K., Kanaoka, A., Matsuo, S., and Minowa, T. (2013) Risk visualization and alerting system: Architecture and proof-of-concept implementation. In: *SESP'13*. 2013, ACM, pp. 3 -10.

[34] OVAL [Online]. Available at: http://oval.mitre.org.

[35] CVE [Online]. Available at: http://cve.mitre.org. (Accessed: 30 March

2018).

[36] CPE [Online]. Available at: http://nvd.nist.gov/cpe.cfm. (Accessed: 4 February 2018)

[37] Mell, P., Scarfone, K., and Romanosky, S. (2007) *CVSS: a complete guide to the common vulnerability scoring system version 2.0*. [Online]. 2007. Available at: http://first.org/cvss/cvss-guide.html. (Accessed: 18 December 2017).

[38] Allodi, L. and Massacci, F. (2014) Comparing Vulnerability Severity and Exploits Using Case-Control Studies. *ACM Transactions on Information and System Security*, 17(1), pp. 1-20

[39] Holm, H., Ekstedt, M., and Andersson, D. (2012) Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks. *IEEE Transactions on Dependable and Secure Computing*, 9(6), pp. 825-837

[40] Wright, J., McQueen, M., and Wellman, L. (2013) Analyses of two end-user software vulnerability exposure metrics (extended version). *Information Security Technical Report*, 17(4), pp. 173-184.

[41] National Vulnerability Database NVD [Online]. Available at: http://nvd.nist.gov/cpe.cfm

[42] Spanos, G., Sioziou, A., and Angelis, L. (2013) WIVSS: A New Methodology for Scoring Information Systems Vulnerabilities. In: *Proceedings of the 17th Panhellenic Conference on Informatics (PCI)*. 2013, ACM, pp. 83-90.

[43] Joshi, C.,and Singh, U. (2016) Quantitative Information Security Risk Assessment Model for University Computing Environment. In: (ICIT 2016) International Conference on Information Technology. 2016, IEEE, pp. 69-74

[44] Moyo, M., Abdullah, H., and Nienaber, R. (2013) Information Security Risk Management in Small-scale Organizations: A Case Study of Secondary Schools Computerized Information Systems. In: *Conference of Information Security for South Africa*. 2013, pp. 1-6.

[45] Theoharidou, M., Mylonas, A., and Gritzalis, D. (2012) A Risk Assessment Method for Smartphones. *IFIP Advances in Information and Communication Technology*, 376, pp. 443-456.

[46] Gros, S. (2011) Complex Systems and Risk Management. In: *MIPRO*. 2011, pp. 1522-1527.

[47] Samy, G., Ahmad, R., and Ismail, Z. (2010) A Framework for Integrated Risk Management Process Using Survival Analysis Approach in Information security. In: *6th International Conference on Information assurance and Security*. 2010, pp. 185-190.

[48] Jain, M. and Clarke, N. (2010) Web-Based Risk Analysis for Home Users. *Advances in Communications, Computing, Networks and Security*, 7, pp. 151-158.

[49] Ledermuller, T. and Clarke, N. (2011) Risk Assessment for Mobile Devices. *Lecture Notes in Computer Science*, 6863, pp. 210-221.

[50] Alohali, M., Clarke, N., Furnell, S. and AlBakri, S. (2017) Information Security Behavior: Recognizing the Influencers. In: (*SAI 2017) Computing Conference*. 2017, IEEE, pp. 844-853.

[51] Blythe, J., Camp, J., and Garg, (2011) Targeted risk communication for computer security. In: *IUI' 11*. 2011, ACM, pp. 295 - 298.

[52] Martin, N. and Rice, J. (2011) Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, 30(8), pp. 803-814.

[53] Maurer, M., De Luca, A., and Kempe, S. (2011) Using data type based security alert dialogs to raise online security awareness. In: *SOUPS' 2011*. 2011, pp. 1 – 13

[54] Shillair, R., Cotten, S., Tsai, H., Alhabash, S., LaRose, R., and Rifon, N. (2015) Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, pp. 199-207

[55] Furnell, S. and Moore, L. (2014) Security literacy: the missing link in today's online society?. *Computer Fraud & Security*, 2014(5), pp. 12-18.

[56] Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., and Giannakopoulos, G. (2014) The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences*, 147, pp. 424-428

[57] Al-Hadadi, M. and Al Shihani, A. (2013) Smartphone security awareness: Time to act. In: *(CTIT) International Conference for Current Trends in Information Technology*. 2013, IEEE, pp. 166 - 171.

[58] Alarifi, A., Tootell, H., and Hyland, P. (2012) A Study of information security awareness and practices in Saudi Arabia. In: *(ICCIT 2012) The 2nd International Conference on Communication and Information Technology*. 2012, IEEE, pp. 6 – 12

[59] Abawajy, J. (2012) User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), pp. 237-248.

[60] Webb, J., Ahmad, A., Maynard, S., and Shanks, G. (2014) A situation awareness model for information security risk management. *Computers & Security*, 44, pp. 1-15.

[61] Stewart, G. and Lacey, D. (2012) Death by a thousand facts: Criticizing the technocratic approach to information security awareness. *Information Management and Computer Security*, 20(1), pp. 29-38

[62] Shropshire, J., Warkentin, M., and Sharma, S. (2015) Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, pp. 177-191

[63] Gabriel, T. and Furnell, S. (2011) Selecting security champions, Computer Fraud & Security 2011 (8), pp. 8-12

[64] Halevi, T., Lewis, J., and Memon, N. (2013) A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. In: *International World Wide Web Conference (IW3C2)*. 2013, Rio de Janero, Brazil: ACM, pp. 737-744.

[65] Workman, M. (2007) Wisecrackers: a theory grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society of Information Science and Technology, (59) , pp. 662–674

[66] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., and Downs, J. (2010) Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of intervensions. In: *CHI 2010: Privacy Behaviors*. 2010, ACM, pp. 373 – 382

[67] Kruger, H., Flowerday, S., Drevin, L., and Steyn, T. (2011) An assessment of the role of cultural factors in information security awareness. In: *(ISSA) Information Security South Africa*. 2011, IEEE, pp. 1 – 7

[68] Jeske, D., Coventry, L., Briggs, P., and Moorsel, A. (2014) Nudging whom how: IT proficiency, impulse control and secure behavior. *Networks*, 49(18).

[69] Johnston, A., Warkentin, M., McBride, M. and Carter, L. (2016) Dispositional and situational factors: influences on information security policy violations, European Journal of Information Systems, 25(3), pp. 231–251.

[70] Alohali, M., Clarke, N., Li, F. and Furnell, S. (2018) Identifying and Predicting End-user's Risk-taking Behavior. *Information and Computer Security*, Vol. 26, Issue 3, pp. 306-326

[71] Blythe, J. and Camp, L. (2012) Implementing mental models. In: *Security and Privacy Workshops*. 2012, IEEE, pp. 86 - 90.

[72] Wash, R. and Rader, E. (2011) Influencing mental models of security: A research agenda. In: *NSPW' 11*. 2011, ACM, pp. 57 - 66.