Cowley *et al. Security Informatics* (2015) 4:1
DOI 10.1186/s13388-015-0016-x

Security Informatics
a SpringerOpen Journal

RESEARCH Open Access

Factors influencing network risk judgments: a conceptual inquiry and exploratory analysis

Jennifer Cowley[1*], Frank L. Greitzer[2†] and Bronwyn Woods[1†]

Abstract

Effectively assessing and configuring security controls to minimize network risks requires human judgment. Little is known about what factors network professionals perceive to make judgments of network risk. The purpose of this research was to examine first, what factors are important to network risk judgments (Study 1) and second, how risky/safe each factor is judged (Study 2) by a sample of network professionals. In Study 1, a complete list of factors was generated using a focus group method and validated on a broader sample using a survey method with network professionals. Factors detailing the adversary and organizational network readiness were rated highly important. Study 2 investigated the level of riskiness for each factor that is described in a vignette-based factor scenario. The vignette provided context that was missing in Study 1. The highest riskiness ratings were of factors detailing the adversary and the lowest riskiness ratings detailed the organizational network readiness. A significant relationships existed in Study 2 between the level of agreement on each factor's rating across our sample of network professionals and the riskiness level each factor was judged. Factors detailing the adversary were highly agreed upon while factors detailing the organizational capability were less agreed upon. Computational risk models and network risk metrics ask professionals to perceive factors and judge overall network risk levels but no published research exists on what factors are important for network risk judgments. These empirical findings address this gap and factors used in models and metrics could be compared to factors generated herein. Future research and implications are discussed at the close of this paper.

Keywords: Perceived risk; Network risk judgments; Network risk; Network security

Introduction

An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [1]. All information systems, which we use interchangeably with the term networks, have inherent network-related risks that cannot be eliminated completely because of operational resource constraints. Risks, defined as "the possibility of loss, injury, or other adverse or unwelcome circumstance" [2], must then be prioritized based on the relative risk level and addressed according to the feasibility of mitigation strategies given both context and resource constraints. Network professionals must evaluate risk throughout the network lifecycle but we focus on risk evaluation during network design and control configuration.

Within the U.S. Department of Defense (DoD) and civilian government networks, organizations must undergo a network certification process— i.e., ISO27000 series (information security standards published jointly by the International Organization for Standardization, ISO, and the International Electrotechnical Commission, IEC) and NIST 800 series [3])—to evaluate network risk. This process of certification involves a designated approving authority (DAA) who engages with the organization's information assurance (IA) officer to determine the organization's network risk level, based on risks identified and control configurations established to address those risks. Some risks are reduced, but not eliminated, through the implementation of various security controls—i.e., management, operational, and technical safeguards or countermeasures employed within an information system to protect the confidentiality, integrity, and availability of the system and its information (a listing of such controls is

*Correspondence: jcowley@cert.org
†Equal contributors
[1]Carnegie Mellon University Software Engineering Institute, CERT Division, 4500 Fifth Avenue, Pittsburgh, Pennsylvania 15213, USA
Full list of author information is available at the end of the article

found in [1]). Ultimately at the end of the certification process, the DAA certifies that the network, with certain controls implemented, meets an acceptable standardized level of network risk.

This network risk certification process, which requires the perception and judgment of network risk, is difficult to standardize across network professionals because in part, different people believe that different factors are important to judgments of risk ([4,5]). A factor is a perceived circumstance, event, influence, fact, etc. that is related to a particular outcome. Both risk perception and judgment can be influenced by network context ([6,7]), which we operationally define as perceivable factors physically and temporally surrounding an event or circumstance (e.g., the organizational policies, the types of adversaries targeting that organization, the types of adversaries, etc.). With respect to judgments of network risk, little is known about what factors are consistently important and unimportant to network professionals like the DAA and IA officers. Guidelines included in network risk metrics for assessing and assigning risk levels are often generic and not tailored to the conditions and contexts of a given network. Consequently during the decision process, individuals like the DAA may have to ignore certain network attributes not covered in the guidelines or ignore the guidelines altogether. Under circumstances where guidelines cannot be clearly applied, the DAA most likely relies on his/her own perceptual capabilities, work experiences, etc. to judge the network risk level, yet little prior research has investigated exactly what factors are actually being considered. Using a mixed-method approach [8] that combines qualitative and quantitative research methods to achieve study objectives, we attempted to identify and validate the factors people believe are most important to network risk judgments.

The challenges with judging network risk levels are due in part to the semantic complexity of the term itself. Underlying this semantic complexity is the lack of an agreed upon definition of risk from professionals in industry and academia ([6,9]). Consequently, risk miscommunications may arise [6] because interlocutors may have different semantic meanings of the term, risk. Risk is a psychological construct [10], an idea constructed in the human mind from the aggregation of dimensions or categories of abstract or tangible perceived phenomenon. The dimensions constituting network risk that we are familiar with include likelihood, vulnerability, resilience, impact, etc. but it is not clear whether network professionals all believe the same dimensions comprise network risk. Dimensions can be derived from perceived factors that include environmental information, past experiences, and other psychological phenomena such as attitudes and belief systems [6]. For example, a "likelihood" dimension of the network risk construct might be driven by perceived environmental factors and historical experience factors indicating the "likelihood" of successful implementation of security controls prior to an attack. The risk research literature provides varying definitions of risk or perceived risk across different domains (e.g., [11-14]) but no consensus exists about the dimensions underlying risk in general or factors used to construct these dimensions ([6,15-21]). We conjecture that a relationship exists between how network risk is defined, what underlying dimensions are important to a network risk definition, and the relevant dimensional factors used in judgments of network risk. Investigating these dimensions and relevant factors might offer clues to how network risk is defined by network professionals. To our knowledge, no foundational research exists that documents the network risk dimensions and respective factors important to network professionals who design and secure networks. This is the impetus for our research.

We used an exploratory, mixed-method approach to identify what factors are important and unimportant for risk judgment in general (Study 1) and what factors are commonly and most consistently judged as more safe or more risky (Study 2) across our sample of network professionals. Because no prior research has identified network risk dimensions important to risk judgments in the context of a network, Study 2 was designed to address this. Prior research indicates that risk perception and judgment can be influenced by context ([6,7]). Therefore, we were interested in identifying robust dimensions and respective factors that are not susceptible to the effects of different contexts.

This paper is structured to review each study's objective, the method, the results and conclusions. We close this paper with an overall discussion that includes the implications of our findings, the limitations of our research and future directions.

Study 1: factors that impact network risk perception

Study purpose and research overview

The purpose of Study 1 was (a) to generate a comprehensive list of perceived factors that were relevant to judgments of network risk and (b) to determine which factors were considered most and least important to judgments of network risk. A focus group of cybersecurity professionals first generated a list of relevant factors, which were then validated with a broader sample of cybersecurity and network professionals using an online survey method.

Method

Participants

Focus Group Demographics. Five cybersecurity professionals plus one moderator comprised the focus group. All focus group members were employees at a single organization with a variety of cybersecurity expertise.

The self-reported expertise included acquisition support (1 participant), cyber threat and vulnerability analysis (1 participant), cyber enterprise and workforce management (1 participant), and enterprise threat/vulnerability management (2 participants). No other demographic information of this sample is permitted to be disclosed.

Survey Sampling and Demographics. The target population included cybersecurity and/or network professionals, who either designed, implemented, supported, and/or tested networks for security purposes or who trained individuals to do these functions. We used a snowball sampling technique [22], first soliciting colleagues at our institution for study participation; they subsequently invited others inside and outside our organization. The mean sample age ($n = 38$) was 47 years with a standard deviation (*SD*) of 10.3 years. The mean number of years worked in computer science professions was 13 ($SD = 9.7$), and the mean number of years in their current job was 9 ($SD = 7.7$). We did not require participants to report additional demographic information on the DHS sectors supported. Consequently, we had low response rates for this question and did not report on these questions.

Materials and procedure

Focus Group. During three sequential two-hour meetings spread over the course of a week, we conducted a moderated focus group using a brainstorming and consensus building technique [23] to identify all factors (at any granularity of detail) that impact network risk perception. We did not collect related information about why each factor was important, or why some factors had very specific language; we were just generating a comprehensive list. Focus group discussions about "why" a factor was provided often lead to desultory discussions and long debates about the validity of the factor so we discouraged those discussions. Each factor offered by each group member was then recorded on a single Post-it Note™ and organized taxonomically by the focus group on butcher paper using an affinity diagramming technique [24].

Online Survey. All factors generated in the focus group sessions, regardless of their granularity, were placed in an online survey to assess their validity on a broader sample of network professionals. The purpose of the online survey was to assess the consensus on the importance level of each factor. The survey was hosted by SurveyGizmo™, a browser-based survey design and deployment tool, and it comprised three survey subsections: informed consent, factor ratings, and demographics.

Informed consent was obtained in accordance with ethics guidelines for research with human subjects (Institutional Review Board approval HS12-571). After providing consent, participants read the online instructions and then rated each of the factors, presented in random order, one factor per survey page. Each factor was presented in a standardized sentence structure, bolded for quick identification (e.g., "Generally, how important is <factor> to your overall perception of network risk?"); no additional network information or context was provided. Participants were asked to adjust a slider to reflect a level of importance on a continuum between 0 (not at all important) and 100 (extremely important). If a participant could not understand the meaning of the factor or had no experience with it, this person was instructed to refrain from making a rating and to write "don't know" in a comments box below the factor. After rating all presented factors, participants could suggest additional factors.

Participants then answered demographics questions about (a) job title, (b) job-related expertise, current employer(s), (c) whether their current job supported the US government, military, private industry or whether he/she was a private consultant, and (d) which of the 18 DHS ISAC sector(s) he or she supports (e.g., healthcare, banking, energy). The order of the demographics questions was not randomized. Survey participants were financially compensated with a $15 gift card at the close of the survey.

Results

This section first discusses common distributions of ratings for each factor and then compares the factor means. All factors identified by the focus group and used in the online survey are listed in Additional file 1: Table SA-1, for quick reference.

Participants did not typically use the response scales consistently (e.g., some use the entire range of the response scale while others use a small portion) so we characterized these first. The mean importance ratings obtained from our 38 survey participants ranged from 38.8 to 83.5 on the 0 to 100-point scale. Three common distributions of factor ratings (for Factors 8, 5, and 51) are shown in Figure 1: unimodal, bimodal and multimodal. Factor 51 (The maturity of the organization's system capabilities for network defense), an example unimodal distribution, has a high level of agreement with most ratings clustered at the high level, indicating that this factor is very important to most participants. Factor 8 (whether the facility uses "SCADA" supervisory control and data acquisition systems) has a bimodal response distribution because scores were clustered around the low or less important end of the scale and around the high or more important end of the scale. Scores for Factor 5 (whether the network is for the military, government, or civilian sector) are distributed across the range of importance ratings. The Additional file 1: Table SA-2 lists all factors, rank-ordered in descending order according to mean importance ratings, and provides density plots of the rating distributions of each factor. Inspection of all density plots for each factor indicates that 27 factors have

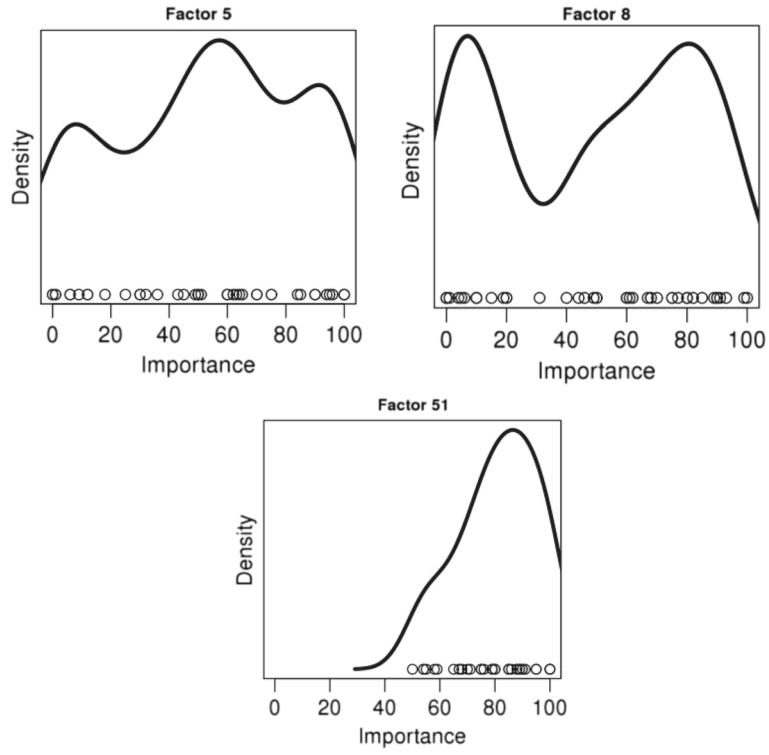


Figure 1 Representative density plots of importance ratings for three factors. Note: The y-axis is the density of responses, and the-x axis is the importance ratings given by participants. Each rating provided by a single participant is represented by a circle along the x-axis, and the curve is the estimated density or probability distribution of ratings for the population (Study 1).

roughly unimodal distributions, 16 factors have roughly bimodal distributions, and the remaining 26 factors have multimodal distributions.

Table 1 provides five factors with the highest mean importance ratings and five factors with the lowest mean importance ratings. The highest rated factors detailed the adversary capabilities and the complexity of the organization's network defense. For example, the factor with the highest mean importance rating was the adversary's knowledge about the organization's deployed network and security technologies (Factor 18, rank = 1). Other highly-rated factors include the skill of the adversary (Factor 31, rank = 3), how desirable the information on the network is to the adversary (Factor 63, rank = 6), whether the adversary has access to information needed to stage an attack (Factor 28, rank = 11), and whether the attack is persistent or casual (Factor 2, rank = 23).

The standard deviations (*SDs*) of the importance ratings (also shown in Additional file 1: Table SA-2) were computed to assess agreement across participants. Table 2 shows the five factors with the least inter-subject agreement (highest *SDs*) and the five with the most inter-subject agreement (lowest *SDs*). By comparing Tables 1 and 2, we note that three of the five factors with the most inter-subject agreement (Factors 18, 45, and 51) were also deemed to be among the most important factors. We assessed whether a relationship existed between the level of importance of each factor (mean importance rating) and the agreement (*SDs*) and no linear relationship was found.

To determine whether dimensions emerged from our data, we used an affinity diagramming method to hierarchically classify the factors generated by the focus group. Three broad categories or dimensions emerged and were named by the research staff after reviewing each the underlying factors of each dimension (see Figure 2): (1) organization hosting the network, (2) threat/adversary, and (3) contractors (prime contractor, sub-contractors). Specific factors mapped to these dimensions were identified in Additional file 1: Table SA-1. An exploratory analysis revealed that of the ten highest-ranked factors, only one was associated with contractors (Factor 1), four were related to the adversary/threat (Factors 7, 18, 31, and 63), and five were associated with the organization (three of these five organizational factors are related to the network environment—Factors 23, 51, and 66). Also, of the ten factors with the lowest rankings, none were associated with the adversary/threat; five were associated with contractors and five with the organization (the low-ranking organizational factors are related to programmatic, policy, and workforce factors—none are associated with network

Table 1 The five least important and five most important factors rated across participants (Study 1, n = 38)

	Factor #	Mean	SD	Factor description
Least Important	30	38.8	29.5	The perceived organizational allegiance (purchases predominantly domestic brands of hardware/software versus purchases foreign brands)
	39	39.6	32.2	Different methods of paying the contractor (e.g., fixed price versus cost plus) to your perception of risk? Fixed price: Payment is a flat fee that must meet predetermined list of requirements. Cost plus: Payment is not flat fee, but it scales over time to cover unforeseen costs of meeting predetermined requirements.
	49	40.6	30.5	The presence or absence of an organization's fear-driven responsiveness to threat
	44	41.8	30.5	The open- or closed-source protection technology used by your organization
	25	42.0	30.9	The recertification cycle (e.g., short versus long) as a constraint effecting the ability to secure the organization's network before an attack
Most Important	66	79.9	21.4	The complexity of the organization's systems and/or networks that makes it easy or difficult to secure
	45	80.5	13.7	The organization's response to threats (proactively planned for an attack versus reactively responded to an attack)
	31	80.8	23.3	The level of skill the adversary has (e.g., professional or amateur)
	51	81.1	14.3	The maturity of the organization's system capabilities for network defense
	18	83.5	17.4	The adversary's knowledge (e.g., high versus low knowledge) about the organization's deployed network and security technology

environment). Thus, factors associated with the adversary/threat and those associated with the organization's network environment appeared to be ranked high in importance; factors associated with contractors tend to be ranked lower in importance, as do other general organizational factors unrelated to the network environment. This is shown in Figure 3, which was generated to assess the relationship between dimensions and risk judgments. The bar chart in Figure 3 displays the percentages of factors in each of the three dimensions that were rated as high (top 1/3), medium (middle 1/3) and low (bottom 1/3) importance. The organization dimension was populated by the highest number of factors compared to the other two dimensions. The matrix in Figure 3 breaks down counts by dimension and level of importance. The highest rated factors (14) and most of the lowest rated factors (13) involved the organization. To assess whether there was a significant association between factor dimension and level of importance, a chi square test of association was conducted and found to be non-significant ($\chi^2(4) = 8.99, p = 0.06$).

Participants were asked whether any important factors needed to be added to our list and these were suggested:

- Does the organization support "doing the right thing" when the situation warrants?
- Morale of the IT, security, and general staff?

Table 2 Factors with the five highest and five lowest standard deviations of importance ratings (Study 1, n = 38)

	Factor #	SD	Mean	Factor
High SDs (Low Agreement)	8	34.0	48.3	Whether the facility uses SCADA systems
	5	32.4	53.3	Whether the network is for the military, government, or civilian sector
	39	32.2	39.6	The different methods of paying the contractor (e.g., fixed price versus cost plus) to your perception of risk?
	21	31.6	59.6	The information types that make up the network contents of your organization
	34	31.5	45.5	The ease (e.g., low versus high ease) of finding U.S.-born personnel instead of foreign-national personnel to fill network security positions within the organization
Low SDs (High Agreement)	45	13.7	80.5	The organization's response to threats (proactively planning for an attack versus reactively responding to an attack)
	51	14.3	81.1	The maturity of system capabilities for network defense
	18	17.4	83.5	The adversary's (level of) knowledge (e.g., high versus low) about the organization's deployed network and security technology
	11	19.3	78.8	Whether the organization has a disaster recovery plan
	12	19.3	70.7	The past performance of the organization's hired contractor

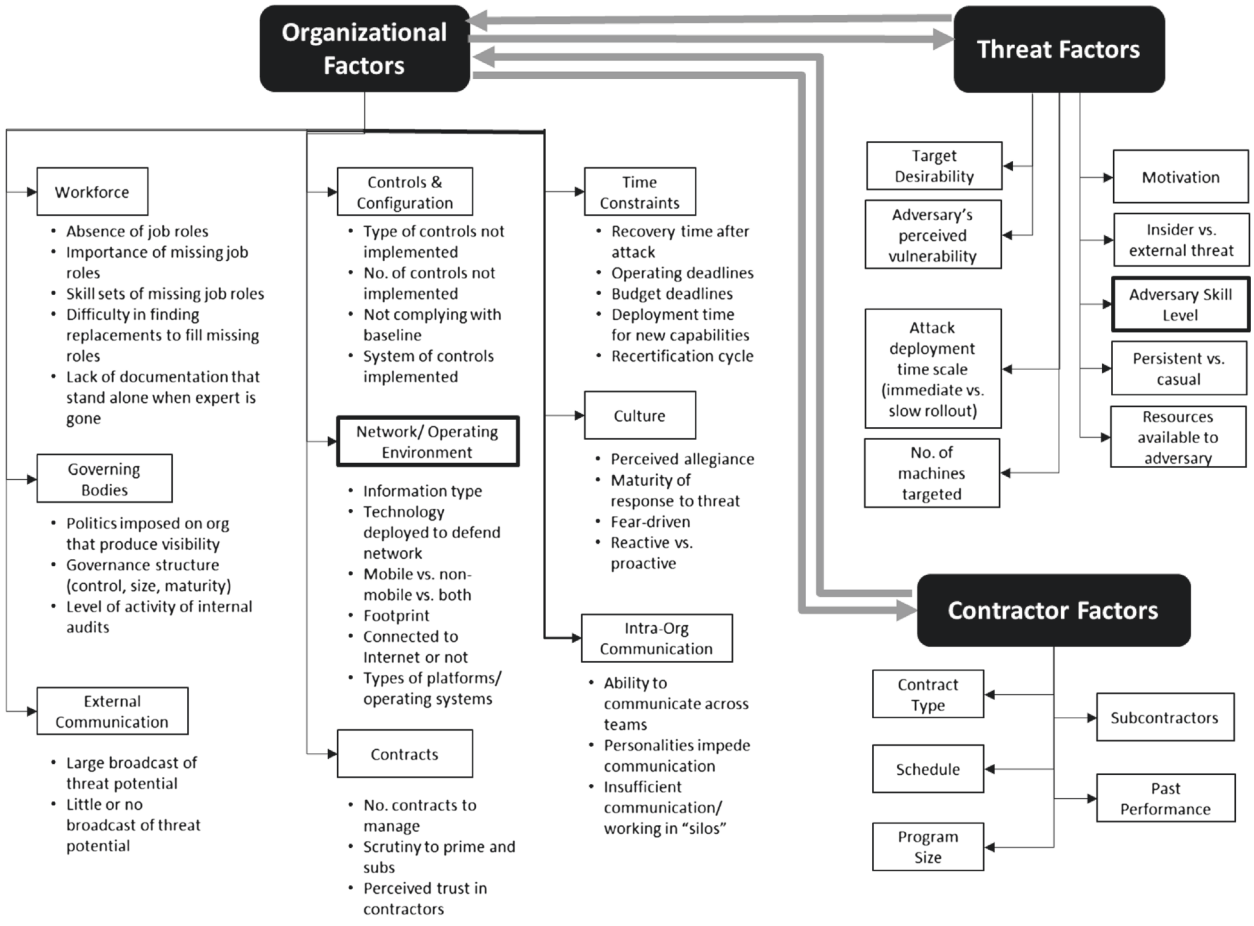


Figure 2 Taxonomy developed based on focus group contributions. Study 1; not all details shown due to space limitations.

- Access to historical intrusion/failure data
- Commitment to IT hygiene
- The presence or absence of a solid knowledge management system.

Discussion

A focus group of network security professionals generated a comprehensive list of factors considered relevant to network risk perception. Our survey results indicated that factors relating to the adversary or to the complexity of the organization's network defense were considered most important. We assessed whether a relationship existed between the level of importance (importance ratings) and the level of agreement *SDs*) amongst our sample participants. While a statistically significant linear relationship between *SDs* and mean ratings of all factors did not exist, the five most agreed-upon factors (lowest *SDs*) were also judged as relatively more important [mean ratings between 70.7 and 80.5]. Three emergent dimensions of factors were found (organization, adversary and contractors) in the absence of context.

The importance of each of our 69 factors was assessed but we could not ascertain whether each factor was safe or risky or whether context changes the emergent dimensions of factors. This became the impetus for the second study.

Study 2: context and network risk perception

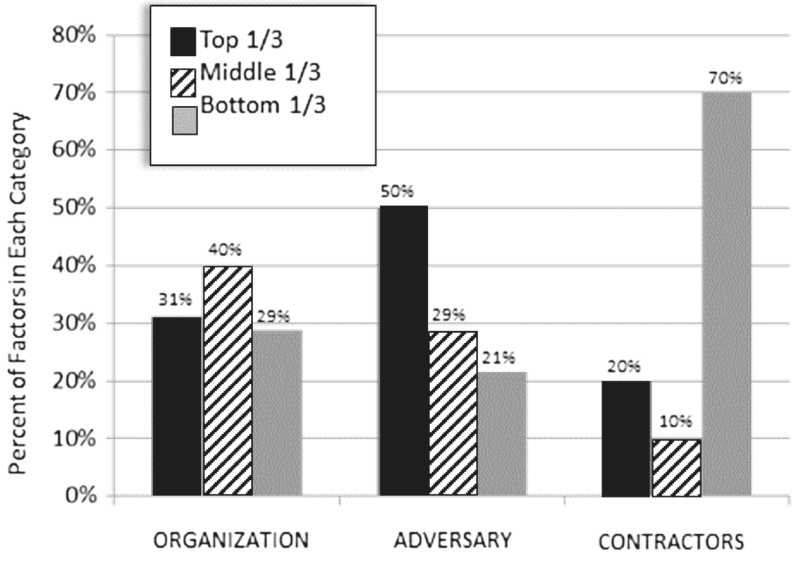
Study purpose and research overview

We used a subset of factors from our original list of 69 factors and analyzed the degree of riskiness or safeness of each. Given the lack of contextual information related to each factor in Study 1, our subset of factors was analyzed using a vignette-based factor scenario method to provide context.

Method

Participants

The target population comprised network professionals versed in the practices of cybersecurity. As shown in Table 3, the 105 participants who completed the survey represented a variety of software engineering, IT



Importance Category	Factor Dimension: ORGANIZATION	ADVERSARY	CONTRACTORS	Total
No. Ranked in Top 1/3	14 (31%)	7 (50%)	2 (20%)	23
No. Ranked in Middle 1/3	18 (40%)	4 (29%)	1 (10%)	23
No. Ranked in Bottom 1/3	13 (29%)	3 (21%)	7 (70%)	23
Total:	45	14	10	69

Figure 3 Relationship between factor dimensions and importance ratings. Percentages of factors in three factor dimensions that ranked in the top, middle, and bottom third in overall importance (Study 1).

management, and information security occupations. The overall mean number of years spent in the computer science professions was 9.6 (SD = 7.6) with a range between 1 and 36 years. We did require participants to report additional demographic information on the Department of Homeland Security (DHS) critical infrastructure sectors supported. The top five DHS sectors participants self-reported to support were Information technology (62), Academia (21), Communications (18), Banking & Finance (17), and Public health (11). Five supported the military, 15 supported the government and 11 were contractors.

Materials and procedures

Three vignettes were generated to represent different network contexts: Vignette 1 described a hospital network, Vignette 2 described a military network, and Vignette 3 described a software development firm network. The context of each vignette differed on attributes like the history of the network and adversarial activity, how the network is manned, the type of information stored on that network and how the network is controlled and configured. Immediately after the participant read the vignette, he/she rated the overall network risk level using a slider (0 = low risk and 100 = high risk) and then offered a ranking (low, medium, or high network risk) according to the NIST SP800-30 guidance [3]. Then, ratings on individual factors were solicited. Originally, we designed the vignettes to depict factors using a few descriptive sentences to depict each factor, but in our survey beta testing, respondents believed that the factors were not the ones we originally intended. Instead, participants believed the main idea of each descriptive sentence was a single factor. Therefore, we obtained ratings for each sentence's main idea using a bipolar response scale between 0 = extremely safe and 100 = extremely risky. A rating of 50 was labeled neither safe nor risky.

Table 3 Frequencies of categories of self-reported job titles (Study 2, n=105)

Job category	Definition	Examples	Number of participants
Analyst	Analyst is a programmer, developer, implementer or other person who provides solutions to customer problems.	Applications security analyst, IT specialist, network systems specialist	34
Architect	Architect is a designer who develops system specifications and balances system-wide tradeoffs.	Network security architect, network architect	7
Engineer	Engineer is a senior developer with some design expertise.	Network engineer, information security engineer,	30
Manager	Manager is responsible for allocating resources to projects and meeting schedules.	Program manager, risk manager, sr. IT manager	12
Director	Director oversees a department or company.	Directory of engineering, director of research, director of IT, CSO	11
Other	"Other" includes students and non-IT-related positions.	Student, recreation assistant	11

SurveyGizmo™ hosted the online survey, which was divided into three sections: informed consent, vignette scenarios, and demographics (job title, the DHS critical infrastructure sectors supported, whether the person was working for the government, military, academia or in training). Informed consent was obtained in accordance with ethics guidelines for research with human subjects (Institutional Review Board approval HS12-571). After providing informed consent, each participant was randomly assigned to one of three vignettes using the survey randomizing tool. Each participant reviewed only one vignette. After reviewing a vignette and providing ratings, participants answered a set of un-randomized demographic questions and were awarded a $20 compensatory Amazon gift card.

Results

Exploratory data analysis of overall risk ratings and rankings

Figure 4 summarizes the vignette risk ratings and risk rankings. In the boxplot on the left, the x-axis represents the vignette number (1 = hospital network, 2 = military and 3 = software development firm) and the y-axis represents the risk ratings. The stacked bar chart on the right shows, for each of the vignettes on the x-axis, the frequency of participants that ranked the risk as either low, medium or high. As shown in the boxplot on the left, Vignette 2 had the highest mean risk rating denoted by the horizontal bar in the middle of the box; but the mean ratings were not significantly different. Though participants believed Vignettes 1 and 3 were relatively less risky, the stacked bar chart on the right of Figure 4 indicates

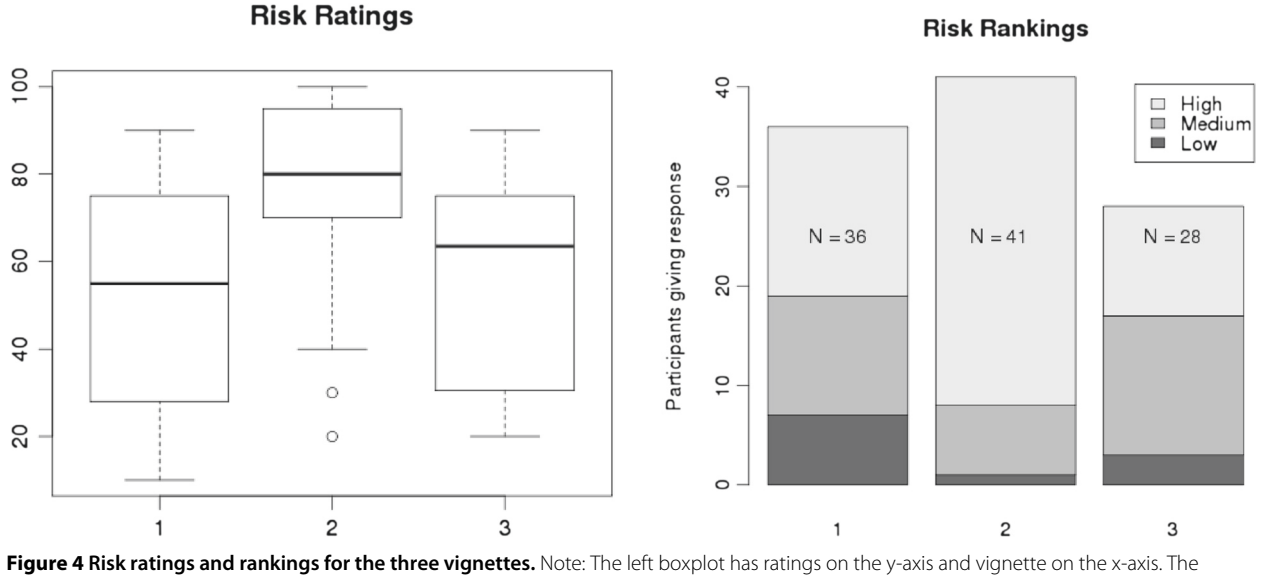


Figure 4 Risk ratings and rankings for the three vignettes. Note: The left boxplot has ratings on the y-axis and vignette on the x-axis. The stacked bar chart displays counts on the y-axis and vignette on the x-axis. The number of participants who read each vignette varied, as indicated by the labels on the bars (Study 2, n = 105).

that participants did not rank any of the vignettes as predominantly low-risk.

Factor grouping by risk impact

One of the goals of Study 2 was to determine which factors, described by certain contextual features, were perceived as risky or safe. We used Bonferroni corrected t-tests to identify factors affecting on risky/safe ratings (i.e., tests conducted against the null hypothesis that population risky/safe means were 50). Those factors with a corrected p-value above 0.05 were removed from further consideration. We then divided the remaining factors (those with mean ratings significantly different from 50) into four groups based on their median scores: VERY SAFE (median rating below 30) includes factors such as Machines are not connected to both the private network and the internet; SOMEWHAT SAFE (median rating between 30 and 45) includes factors such as The IT staff are fully trained; SOMEWHAT RISKY (median rating between 55 and 72) includes factors such as All patient records are digitized; and VERY RISKY (median rating above 72) includes factors such as Hackers in the past few weeks have been attacking various medical centers nationwide. The factors with the median ratings between 46 and 54 were not included in Table 4 because they were not significantly different from 50. Table 4 lists the factors in each of these groups, along with their median and mean risk scores, *SDs*, and vignettes to which they belong.

Table 5 displays the most agreed upon factors (lowest *SDs*) with respect to the risky/safe ratings and the least agreed upon (highest *SDs*). The values of *SDs* for these 85 factors, across all three dimensions, ranged from 10.2 to 24.4 (median = 18.05). To assess whether a relationship existed between the number of high vs. low standard deviations and the risky/safe ratings for those factors, we compared the risk levels assigned to factors that exhibited *SDs* below the median (high agreement among respondents) with those that exhibited *SDs* above the median (low agreement across respondents). For risk levels, we used the same categories shown above for Table 4: Safe (Rating $<$ 45), Neutral (45 $<$ Rating $<$ 55), Risky (55 $<$ Rating). Table 6 provides the 2×3 matrix of high/low agreement by safe/neutral/risky importance ratings. The resultant significant chi-square test of association ($\chi^2(2) = 7.06, p = 0.029, n = 85$) indicated that our study participants agreed more about factors that were judged as riskier, compared to those that relate to lower network risk.

Factor groupings based on correlation

One way to summarize the ratings data for each single vignette is to group the ratings into clusters of factors that vary together across participants. Then, determine whether an underlying conceptual or semantic commonality exists amongst a group of factors that cluster; likened to a principal components analysis used with larger sample sizes. If commonalities exist, they may provide clues about 'agreed upon' underlying parameters or dimensions related to network risk judgments.

For each vignette independently, we computed the correlation matrix between all the factors (all pair-wise correlations). We used [1 − *correlation*] as a distance measure and performed hierarchical clustering with the Ward agglomeration method to divide the factors into groups that might be interpreted as dimensions of the perceived risk construct. We chose the number of clusters, k, for each scenario based on examining several heuristics. Other choices of k could be equally valid.

The resultant correlation matrices revealed clusters of factors for Vignettes 1 and 2 with relatively strong correlations within the group and low correlations between factors in different groups. Because no such relationships were observed in Vignette 3, it was not included in further analyses. While the groupings reflect statistical structure in the data, that structure does not always correspond to a semantic representation of single dimensions. When the majority of the constituent factors in a group shared a common semantic interpretation, we adopted this semantic interpretation as a label for a network risk construct dimension. Four labeled dimensions across the two vignettes emerged:

(a) *Information* factors related to the information stored on the network and the consequences of the information being compromised — inferred from Vignette 1 (hospital network)
(b) *Infrastructure* factors related to the infrastructure of the network and the compliance of the network with established protocols.)—inferred from Vignette 1 (hospital network)
(c) *Personnel Skill* factors related to the skill and training of network personnel — inferred from Vignette 2 (military network)
(d) *Adversary Skill* factors related to the skill, resources, and motivation of the adversary — inferred from Vignette 2 (military network).

Table 7 lists the factors (with associated mean risk ratings and *SDs*) in each of these emergent dimensions. Also shown in Table 7 (last column) is the risky/safe grouping (VS = Very Safe, SS = Somewhat Safe, SR = Somewhat Risky, and VR = Very Risky) to which the factor belongs (if any). We note that of the four dimensions of the perceived risk construct, the adversary skill dimension contains the highest percentage of risky (SR or VR)

Table 4 Factors organized by risky/safe ratings (Study 2)

Vignette	Median risk	Mean risk	SD	Factor
				Very safe (Median risk rating <30)
1	26.0	30.0	15.2	The hospital recently installed additional emergency electrical generators.
1	28.5	31.9	18.4	A disaster recovery plan has been implemented.
1	24.5	24.2	18.5	Machines are not connected to both the private network and the internet.
1	29.0	32.1	19.0	Results of the audit meet or exceed best practices for network configuration and maintenance.
1	25.0	32.8	20.8	The recovery effort from a natural disaster is expected to be rapid.
2	25.0	26.0	20.8	The network is a self-contained, segregated, and air-gapped network.
2	30.0	34.6	20.9	The IT staff man the network 24/7.
3	25.0	27.1	13.4	The networks are fully manned with very little employee turnover.
3	30.0	30.7	17.7	IT staff is highly trained in their area of expertise via outside training firms and local universities.
3	24.0	24.7	18.0	The chief strategy officer (CSO) has put in place a dedicated controls management team whose job is to make sure that the security controls implemented are the most effective ones possible whether or not they are required for compliance.
3	29.5	29.0	19.8	The CSO is passionate about security.
				Somewhat safe (Median risk rating between 30 and 45)
1	32.0	30.7	16.6	The personnel manning facilities are competent.
1	33.5	31.1	17.1	The IT department is adequately staffed.
1	42.0	36.5	18.0	IT had a yearly audit due to HIPAA requirements.
1	34.5	35.8	19.4	All digitized records are stored and processed on a private network.
2	35.0	36.7	15.9	An audit was recently passed.
2	35.0	35.1	18.4	The network is in full compliance with the DoD.
2	34.0	36.4	20.4	The IT staff are fully trained.
3	35.5	33.9	17.5	85% of these employees have been employees of the company for 15 years or more.
				Somewhat risky (Median risk rating between 55 and 72)
1	56.0	58.0	11.6	The recent legislation on the reformation of the national health care system
1	58.5	62.6	14.0	Various adversarial organizations have growing concerns over the lack of medical record privacy because of the legislation.
1	69.5	69.8	15.9	The type of data the hospital handles
1	65.5	64.6	16.2	All patient records are digitized.
1	70.0	66.8	16.6	End users have Windows machines.
1	65.0	68.2	17.3	It (the network) involves a large hospital.
1	59.5	63.1	17.4	The hacker's intent was to motivate another reformation of the national health care system.
2	70.0	68.5	20.2	The network is within a small geographical region near a war zone.
2	65.0	67.1	22.1	The network is heterogeneous with Windows, UNIX, and proprietary military operating systems.
3	68.5	66.5	10.2	The organization has 20 offices worldwide.
3	56.0	61.3	13.9	The software development firm has 13,000 employees.
3	70.0	71.5	14.1	Competition is fierce in the business intelligence domain.
3	60.0	63.8	14.2	Offices are located in North America, South America, Asia, Europe, and Australia.
3	72.0	73.8	14.9	It took a couple of years to recover from these two incidents.
3	70.0	74.2	17.8	Clients are from the government military and commercial sectors of 135 countries.
3	71.0	69.9	18.9	The intranet hosts a database of technical reports, proprietary design information, social collaboration tools, email servers, etc.

Table 4 Factors organized by risky/safe ratings (Study 2) *(Continued)*

				Very risky (Median risk rating >72)
1	76.0	74.9	18.1	A prolonged outage of digital recordkeeping could cause significant damage to the hospital's ability to serve its patients.
1	82.5	78.6	18.5	Release of patient care information puts the hospital in legal liability.
1	75.0	72.9	18.8	Hackers in the past few weeks have been attacking various medical centers nationwide.
1	74.5	73.2	19.1	These attacks in the past few weeks have leaked private patient care information on the internet.
1	75.0	74.4	20.0	These adversarial organizations are persistent and academically capable of executing an attack.
1	77.5	75.9	22.5	Release of patient care information damages the hospital's reputation.
1	75.0	70.6	24.0	Release of patient care information violates HIPAA regulations.
2	95.0	92.6	10.2	The primary adversary has excellent offensive cyber skills equal to or better than 90 existing nation states.
2	90.0	87.5	12.1	The primary adversary is well funded.
2	100.0	92.2	12.1	Malicious activity has been noted on the network in the past six months since wartime operations intensified in this region.
2	95.0	88.8	13.9	The adversary was likely trained by the U.S. government in the past two years.
2	95.0	87.7	14.8	The adversary is highly motivated.
2	90.0	86.2	14.9	The adversary is deeply interested in U.S. troop positioning.
2	80.0	78.8	16.4	The network has Windows systems.
2	85.0	83.1	16.9	The primary adversary is a nation state.
2	90.0	84.3	17.1	The network stores highly sensitive data related to enemy versus U.S. troop positioning and high-value target location information.
2	80.0	77.0	17.3	This network stores and processes time-sensitive intelligence information.
2	87.0	80.4	18.8	The information stored and processed on this network includes Top Secret SEI 5 Eyes NOFORN information.
2	77.0	69.9	24.1	This involves a classified military network.
3	77.5	82.5	12.6	Competitors have sophisticated well-funded espionage teams to steal competitive information.
3	75.0	77.9	14.8	Almost all employee machines have access to both the internet and intranet.

factors (90%), while the infrastructure dimension contains the highest percentage of safe (VS or SS) factors (60%).

Conclusion

As in Study 1, there tended to be higher agreement on the most risky factors. For example, of the 13 factors with the most agreement in ratings (lowest *SDs*), nine were judged as risky while two were rated neutral and one was rated safe. On the other hand, for the 16 least agreed upon factors (high *SDs*), no discernable differences were observed in risky/safe ratings. Moreover, factors that were associated with the adversary/threat tended to be rated as more risky in general. Of the 13 factors with the most agreement in ratings (lowest *SDs*), six involved descriptions of the adversary (five were rated as very risky and one was rated as somewhat risky). Factors relating to the organization's network infrastructure tended to be associated with lower risk as well. The semantic groupings, or dimensions, derived from inter-factor correlations have similar trending as discussed in the preceding paragraph. Of the four emergent network risk dimensions (i.e., information, infrastructure, personnel skill and adversary skill), the highest proportion of the most risky factors comprised the adversary skill dimension (90%) while the highest proportion of the most safe factors comprise the infrastructure dimension (60%). Somewhat safe factors often comprise the personnel skill and infrastructure dimensions and somewhat risky factors span all four dimensions.

Overall discussion

Study 1 initially used a focus group method to produce a list of possible factors believed to influence network risk judgments and then used an online survey method to investigate the importance of these factors with a broader sample of network professionals. Study 1 did not ask participants how risky each factor was, just the level of importance. Study 2 extended the Study 1 findings by asking network professionals to review one of three vignettes and judge how risky or safe each factor was in the vignette. We understood that network risk judgments are difficult to

Table 5 Lowest 15 and highest 15 standard deviations of factor importance ratings (Study 2)

SD	Vignette	Median risk	Mean risk	Factor
				Low SDs (High Agreement)
10.2	2	95.0	92.6	The primary adversary has excellent offensive cyber skills equal to or better than 90 existing nation states.
10.2	3	68.5	66.5	The organization has 20 offices worldwide.
10.3	1	50.0	50.7	These adversarial organizations are not financially well funded.
10.9	1	50.0	45.2	Database is Linux based for large-scale processing and storage.
11.6	1	56.0	58.0	The recent legislation on the reformation of the national health care system.
12.1	2	90.0	87.5	The primary adversary is well funded.
12.1	2	100.0	92.2	Malicious activity has been noted on the network in the past six months since wartime operations intensified in this region.
12.6	3	77.5	82.5	Competitors have sophisticated well-funded espionage teams to steal competitive information.
13.4	3	25.0	27.1	The networks are fully manned with very little employee turnover.
13.9	2	95.0	88.8	The adversary was likely trained by the U.S. government in the past two years.
13.9	3	56.0	61.3	The software development firm has 13,000 employees.
14.0	1	58.5	62.6	Various adversarial organizations have growing concerns over the lack of medical record privacy because of the legislation.
14.1	3	70.0	71.5	Competition is fierce in the business intelligence domain.
14.2	3	60.0	63.8	The offices are located in North America, South America, Asia, Europe, and Australia.
14.4	1	50.0	48.2	Neither department has reported adversarial activity in the past that demonstrate a knowledge of the IT infrastructure.
				High SDs (Low Agreement)
20.9	2	30.0	34.6	The IT staff man the network 24/7.
20.9	3	36.5	38.1	These employees are divided into small, highly specialized teams working on one aspect of the network e.g., LDAP server teams, router teams.
21.4	1	50.0	45.4	Records are transferred from one hospital to another manually.
21.4	2	58.0	59.6	The network has various UNIX systems.
21.9	3	50.0	50.6	No targeted attacks in the past few years. Only non-targeted email scams
22.0	1	45.0	40.3	Recordkeeping could convert back to paper.
22.1	2	65.0	67.1	The network is heterogeneous with Windows, UNIX, and proprietary military operating systems.
22.3	2	42.0	41.6	Full recovery is expected to occur quickly.
22.5	1	77.5	75.9	Release of patient care information damages the hospital's reputation.
22.7	3	43.0	45.2	The company uses proprietary languages and tools that are very difficult to exploit.
22.9	2	47.0	48.1	The IT staff are supported by various stable vendor contractors.
24.0	1	75.0	70.6	Release of patient care information violates HIPAA regulations.
24.1	2	77.0	69.9	This involves a classified military network.
24.2	1	66.0	64.9	The back-end servers are unique and housed in a single data center on the hospital premises.
24.4	2	35.0	41.9	The systems running on the network use proprietary military operating systems.

make without contextual information so Study 2 provided contextual information that Study 1 lacked.

Study 2 was designed to help refine our understanding of the factors that were identified as important in Study 1. For example, factors relating to the adversary (knowledge/skill/capabilities) were considered highly important in Study1 and were also associated with higher levels of network risk. Many of these factors detailing the adversary formed the adversary/threat dimension in Study 2. Also, in Study 1, factors detailing the organization were found to have different levels of importance. Study 2 helped us refine our understanding of the organizational factors that were and were not important. Specifically, factors relating to the organization's network infrastructure and

Table 6 Relationship between perceived risk level and agreement (Study 2)

	Safe	Neutral	Risky	*Totals*
Low Agreement (High SD)	17	10	14	41
High Agreement (Low SD)	9	6	26	41
Totals	26	16	40	82

its ability to defend against attacks were relatively more important than others in Study 1 and were associated with lower levels of network risk in Study 2. Both studies had two dimensions in common; threat/adversary and the organization. The two dimensions discovered in Study 2, information and personnel skill, were related to the subset of Study 1 organizational factors that seemed to have high variability in importance ratings. Hence, whether or not context was present, our sample of network professionals believed that dimensions of network risk should include both organizational network infrastructure (the preparedness for attack) and the threat/adversary (the attack). This provides some clues about the dimensions of network risk definitions that network professionals, rather than risk metric designers, endorse.

The finding that network risk judgments are strongly influenced by information about the adversary/threat is important because network certification generally neglects threat/adversary factors. For example, the NIST CVSS v2.10 metric focuses mainly on other factors associated with information, infrastructure, and personnel skill. One reason why the threat/adversary factors were both very important and risky to our study participants is that the existence of unknown, dangerous entities (i.e., the adversary) which cannot be easily perceived and controlled is anxiety provoking. While the factors we provided about the adversary were of known qualities (e.g., the adversary has excellent cyber offense skills, the adversary is highly motivated), the adversary still poses an uncomfortable uncertainty in network defense because one cannot predict when an attack will occur (and by whom), how the attack will be executed, and what the adversary wants. Prior research has indicated that people are generally uncomfortable with uncertainty and typically avoid it [25,26], and when uncertainty cannot be avoided, a fear response is invoked [27]. When fear increases, perceptions of risk also increase [28-30].

Implications

The importance of our results is that we used research methods from the social sciences to devise a list of factors that impact network risk judgments from network professionals. This information is important for risk metric designers who require metric users to subjectively interpret various factors as part of the metric output. Given little information is published on how certain factors were chosen for these network risk metrics, it is possible that these factors were chosen according to the opinions of the risk metric designer rather than the opinions of network professionals. Factors that our sample agrees are more important to risk judgments may not be the factors the metric designer includes; which we detail in the subsequent paragraph. We make the argument herein that network risk is difficult for one person to accurately judge given the technical knowledge diversity required. Therefore, consensus on factors important to risk judgments from a sample of network professionals may inform risk metric designers. In addition, future research on network risk perception and judgment can build upon our findings.

The factors our sample agreed were risky and important to network risk judgments were not necessarily factors included in computed risk models like the NIST CVSS V2.10. For example, the CVSS V2.10 includes factors describing organizational and network readiness rather than the adversarial capabilities. While it could be argued that the NIST CVSS V2.10 metric assess vulnerabilities, the metric is being used for security risk management (http://www.first.org/cvss/cvss-guide). Our research identified drivers for high network risk levels that are missing or not well articulated in this NIST metric: From Study 1, "the adversary's knowledge about the organization's deployed network and security technology" and "the adversary's level of skill (professional vs. amateur)". The importance of these missing factors was confirmed in Study 2 when participants rated the adversary's skill and training as factors that greatly increase network risk levels. Other missing factors that we identified as contributing to risk perception were perceived adversarial motivation, success rate of the adversary exploitation in recent history, and the importance of the targeted data to be exploited. Factors that reliably increase or decrease perceived risk are likely to be important for an accurate computed risk model.

Limitations and future directions

A few limitations are worth mentioning that may have impacted our results. First, the target population in these two studies was difficult to persuade to participate in our studies. Network professionals familiar with adversarial techniques used to penetrate a network, may mistake the emailed survey links for a phishing campaign. Therefore, sampling was challenging, which was reflected in our low sample sizes and consequently, we were limited

Table 7 Emergent network risk dimensions and associated factors (Study 2)

Factor	Mean risk	SD	Risk group
INFORMATION DIMENSION: Features related to the information stored on the network, the adversaries who want that information, and the consequences of the information being compromised. [Vignette #1: Hospital network]			
Recordkeeping could convert back to paper.	40.6	21.8	
Hospital is in a metropolitan area.	56.6	16.1	
Various adversarial organizations have growing concerns over the lack of medical record privacy because of the legislation.	63.1	14.3	
The hacker's intent was to motivate another reformation of the national health care system.	63.1	18.0	SR
All patient records are digitized.	65.0	16.0	SR
It (the network) involves a large hospital.	68.4	17.4	SR
The type of data the hospital handles	68.9	5.9	SR
Release of patient care information violates HIPAA regulations.	71.9	24.1	VR
Hackers in the past few weeks have been attacking various medical centers nationwide.	72.4	9.3	VR
These attacks in the past few weeks have leaked private patient care information on the internet.	74.0	19.2	VR
These adversarial organizations are persistent and academically capable of executing an attack.	74.3	20.6	VR
A prolonged outage of digital recordkeeping could cause significant damage to the hospital's ability to serve its patients.	75.2	18.0	VR
Release of patient care information damages hospital's reputation.	76.2	22.6	
Release of patient care information puts the hospital in legal liability.	79.9	18.0	VR
INFRASTRUCTURE DIMENSION: Features related to the infrastructure of the network and the compliance of the network with established protocols. [Vignette #1: Hospital network]			
Machines are not connected to both the private network and the internet.	24.0	18.5	VS
The hospital recently installed additional emergency electrical generators.	29.6	15.6	VS
The personnel manning facilities are competent.	30.9	17.1	SS
The IT department is adequately staffed.	31.7	17.2	SS
A disaster recovery plan has been implemented.	32.0	18.8	VS
Results of the audit meet or exceed best practices for network configuration and maintenance.	32.0	19.6	VS
The recovery effort from a natural disaster is expected to be rapid.	32.3	21.2	VS
All digitized records are stored and processed on a private network.	36.0	19.9	SS
IT had a yearly audit due to HIPAA requirements.	36.6	18.5	SS
Database is Linux based for large-scale processing and storage.	44.8	11.1	
Records are transferred from one hospital to another manually.	45.3	20.6	
These adversarial organizations are not financially well funded.	50.6	10.2	
The recent legislation on the reformation of the national health care system	58.2	11.9	
Network is connected to programmable logic controllers (PLCs) for the medical equipment to receive test results and to manage and operate the machines. A PLC is a digital computer used for automating electromechanical processes.	59.7	17.4	
The back-end servers are unique and housed in a single data center on the hospital premises.	64.9	24.9	
PERSONNEL SKILL DIMENSION: Features related to the skill and training of network personnel. [Vignette #2: Military network]			
The network is a self-contained, segregated, and air-gapped network.	26.0	20.8	VS
The IT staff man the network 24/7.	34.6	20.9	VS
The network is in full compliance with the DoD.	35.1	18.4	SS
The IT staff are fully trained.	36.4	20.4	SS

Table 7 Emergent network risk dimensions and associated factors (Study 2) *(Continued)*

Factor	Mean risk	SD	Risk group
An audit was recently passed.	36.7	15.9	
The IT staff are well trained at various military schools.	39.2	19.3	
The military installation has a mature emergency operation plan (EOP) and continuity of operations plan (COOP) that comply with the Federal Emergency Management Agency (FEMA) recommendations.	41.0	19.3	
Full recovery is expected to occur quickly.	41.6	22.3	
The systems running on the network use proprietary military operating systems.	41.9	24.4	
The network is within a small geographical region near a war zone.	68.5	20.2	SR
ADVERSARY SKILL DIMENSION: Features related to the skill, resources, and motivation of the adversary. [Vignette #2: Military network]			
The network has various UNIX systems.	59.6	21.4	
The network is heterogeneous with Windows, UNIX, and proprietary military operating systems.	67.1	22.1	SR
The network has Windows systems.	78.8	16.4	VR
The primary adversary is a nation state.	83.1	16.9	VR
The adversary is deeply interested in U.S. troop positioning.	86.2	14.9	VR
The primary adversary is well funded.	87.5	12.1	VR
The adversary is highly motivated.	87.7	14.8	VR
The adversary was likely trained by the U.S. government in the past two years.	88.8	13.9	VR
Malicious activity has been noted on the network in the past six months since wartime operations intensified in this region.	92.2	12.1	VR
The primary adversary has excellent offensive cyber skills equal to or better than 90 existing nation states.	92.6	10.2	VR

in the types of statistical analyses we could conduct. For example, we wanted to relate the risky/safe ratings for each factor to the overall network risk rating of each vignette but the low sample sizes made that impossible. We also wished to assess group differences (military, private industry, government) but again, the sample sizes encumbered that effort. One way to reduce the time burden for study participation was to only require questions that were central to the study objective. Consequently, not all demographics questions were required in both studies, which resulted in low question response rates that could never characterize the sample.

Another limitation is that it is unclear whether our findings reflect the judgments of DAA and IA officers. The process of network certification described in our study may be of little relevance to the broader sample of individuals involved in network defense. The derived judgments and perceptions may not align with those of DAA and IA officers who conduct network certification in the public sector, especially military organizations (the relatively low representation of public sector respondents in Study 2 underscores this limitation). Similarly, construct dimensions derived in our data-driven approach may be a reflection of the views and experience of the participants in our study. While it was impractical for our studies to sample exclusively from personnel responsible for configuring and certifying networks, future research should include validation studies to determine if our results are consistent with judgments obtained from individuals directly responsible for network certification.

In addition, future research should continue to flesh out which factors are significantly risky and safe in various network contexts and why. Our results were intended to serve as a foundation upon which future research and operations can be built. For example, network risk metrics in operations could improve the validity of network risk metrics by including some of our most agreed upon risky and safe factors. Researchers could investigate whether commonly agreed upon dimensions relate to factor perception and definitions of network risk.

Additional file

Additional file 1: Supplemental material for study 1.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
JC conceived, designed, and carried out the studies, oversaw analyses that were performed, and was the primary author of a technical report

documenting the studies. FG supported analyses that were performed, participated in interpreting results and implications of the work, and drafted the version of the manuscript for publication. BW conducted statistical analyses and helped to interpret results. All authors read and approved the final manuscript.

Acknowledgements
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute. No warranty. This Carnegie Mellon University and Software Engineering Institute material is furnished on an "AS-IS" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement. This material has been approved for public release and unlimited distribution. Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University. DM-0001925.

Author details
[1]Carnegie Mellon University Software Engineering Institute, CERT Division, 4500 Fifth Avenue, Pittsburgh, Pennsylvania 15213, USA. [2]PsyberAnalytix, 651 Big Sky Drive, Richland, Washington 99352, USA.

Received: 4 April 2010 Accepted: 11 March 2015
Published online: 10 April 2015

References

1. Joint Task Force Transformation Initiative, National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4.* (Washington, D.C., National Institute of Standards and Technology, 2013). http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
2. Oxford English Dictionary (online). (Oxford/New York, Oxford University Press, 2014). risk, n. http://www.oed.com/view/Entry/166306?rskey=Z0aceK&result=1&isAdvanced=false (accessed November 17, 2014)
3. Joint Task Force Transformation Initiative, National Institute of Standards and Technology (NIST), *Guide for Conducting Risk Assessments (NIST Special Publication 800-30 Revision 1).* (Washington, D.C., National Institute of Standards and Technology, 2012). http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
4. P Slovic, B Fischhoff, S Lichtenstein, in *Perilous progress: Managing the hazards of technology*, ed. by RW Kates, C Hohenemser, and JX Kasperson. *Characterizing perceived risk.* (Boulder: Westview, 1985), pp. 91–125
5. B Fischhoff, SR Watson, C Hope, Defining risk. Policy Sci. **17**, 123–139 (1984). doi:10.1007/BF00146924
6. B Fischhoff, in *Oxford Textbook of Public Health, Fifth Edition.* ed. by R Detels, R Beaglehole, MA Lansang, and M Gulliford. *Risk Perception and Communication.* (Oxford: Oxford University Press, Sage; 2009), pp. 940–952
7. EC Poulton, *Bias in Quantifying Judgments*. (East Sussex, UK: Laurence Erlbaum Associates, Ltd., 1989)
8. JW Creswell, *Mixed-method research: Introduction and application.* In C Ciznek (Ed.), *Handbook of educational policy*. (San Diego, CA: Academic Press, 1999), pp. 455–472
9. O Renn, Three decades of risk research: accomplishments and new challenges. J. Risk Res. **1**, 49–71 (1998). doi:10.1080/136698798377321
10. LJ Cronbach, PE Meehl, Construct validity in psychological tests. Psychol. Bull. **52**(4), 281–302 (1955)
11. T Aven, *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective*. (West Sussex, UK: John Wiley & Sons Ltd, 2003). ISBN 0-471-49548-4
12. LG Epstein, A definition of uncertainty aversion. Rev. Econ. Stud. **66**(3), 579–608 (1999)
13. WW Lowrance, *Of Acceptable Risk: Science and the Determination of Safety*. (Los Altos, CA: William Kaufmann, 1976)
14. A Pollatsek, A Tversky, A theory of risk. J. Math. Psychol. **7**(3), 540–553 (1970)
15. RA Bauer, *Consumer Behavior as Risk Taking.* In RE Karp (Ed.), *Issues in Marketing*. (New York: MSS Information Corporation, 1999), pp. 389–398. ISBN 0-8422-5165-0
16. AH Crespo, IR del Bosque, MMG de los Salmones Sanchez, The influence of perceived risk on internet shopping behavior: A multidimensional perspective. J. Risk Res. **12**(2), 259–277 (2009). doi:10.1080/13669870802497744
17. GR Dowling, Perceived risk: the concept and its measurement. Psychol. Mark. **3**(3), 193–210 (1986). doi:10.1002/mar.4220030307
18. HG Gemünden, Perceived risk and information search: a systematic meta-analysis of the empirical evidence. Int. J. Res. Market. **2**(2), 79–100 (1985)
19. YY Haimes, On the complex definition of risk: a systems-based approach. Risk Anal. **29**(12), 1647–1654 (2009). doi:10.1111/j.1539-6924.2009.01310.x
20. CA Ingene, MA Hughes, *Risk management by consumers.* In EC Hirschman (Ed.), *Research in Consumer Behavior, Vol. 1*. (Greenwich, CT: Emerald Group Publishing Limited, 1985), pp. 103–158
21. I Ross, Perceived risk and consumer behavior: a critical review. Adv. Consum. Res. **2**(1), 1–19 (1975)
22. P Biernacki, D Waldorf, Snowball sampling: problems and techniques of chain referral sampling. Sociol. Methods Res. **10**(2), 141–163 (1981). doi:10.1177/004912418101000205
23. DE Hartley, *Job Analysis at the Speed of Reality*. (Amherst, MA: Human Resource Development Press Inc., 1999)
24. H Beyer, K Holtzblatt, *Contextual design: defining customer-centered systems*. (Oxford, UK: Elsevier;1998)
25. G Hofstede, *Culture's Consequences: International Differences in Work-Related Values*, (Beverly Hills, CA: SAGE Publications, 1980)
26. PW Dorfman, JP Howell, in *Advances in International Comparative Management.* ed. by EG McGoun. *Dimensions of National Culture and Effective Leadership Patterns: Hofstede Revisited.* vol. 3 (Greenwich, CT: JAI Press, 1988), pp. 127–150
27. G Hofstede, *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations, 2nd Edition.* (Thousand Oaks, CA: SAGE Publications, 2001)
28. B Fischhoff, et al., How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. Policy Sci. **9**, 127–152 (1978)
29. JS Lerner, RM Gonzalez, DA Small, B Fischhoff, Effects of fear and anger on perceived risks of terrorism a national field experiment. Psychol. Sci. **14**(2), 144–150 (2003)
30. P Slovic, E Peters, Risk perception and affect. Current directions in psychological science. **15**(6), 322–325 (2006)