J Comput High Educ (2013) 25:49–67
DOI 10.1007/s12528-013-9067-5

# Risks and uncertainties in virtual worlds: an educators' perspective

**Fariborz Farahmand · Aman Yadav · Eugene H. Spafford**

Published online: 15 March 2013


**Abstract** Virtual worlds present tremendous advantages to cyberlearning. For example, in virtual worlds users can socialize with others, build objects and share them, customize parts of the world and hold lectures, do experiments, or share data. However, virtual worlds pose a wide range of security, privacy, and safety concerns. This may lead educators to become (or not) apprehensive of the virtual worlds in using and adapting them as learning technologies. This study examined how educators perceive risks and uncertainties in virtual worlds. We also investigated how educators' level of use of virtual worlds influences their risk perception level. Our results indicate a divergence between risk perception and reality in the virtual worlds. We use the seminal risk perception model developed by Fischhoff and his colleagues, and our revision to this model to explain these results. Finally, we discuss implications of our research for education management, and make recommendations to educators and policy makers who consider using virtual worlds as a learning technology.

**Keywords** Computer uses in education · Risk management · Security and privacy protection · Virtual reality

## Introduction

The rich domains of virtual worlds provide new environments, new economies, and new institutions. Gartner (2009) predicted that by the end of 2012 80 % of active Internet users would have a second life in a virtual world and that major enterprises

F. Farahmand (✉) · E. H. Spafford
Purdue University, Recitation Building, 656 Oval Drive, West Lafayette, IN 47907, USA
e-mail: fariborz@purdue.edu

A. Yadav
Purdue University, 100 N. University St, West Lafayette, IN 47907, USA

would find value in participating in these virtual venues. These numbers indicate that human interaction with the virtual is expected to approach some of the extremes seen in popular science fiction works such as True Names (Vinge 1981) and Halting State (Stross 2007).

The National Science Foundation indicated that virtual worlds have the potential to play a major role in education and training as students can interact with content in virtual communities (NSF 2008). In these environments, learners can create an avatar—the computer representation of the user—to represent themselves, which they use to move around inside a virtually rendered world space shared with thousands of other avatars. They can socialize with others; build objects and share them; customize parts of the world; hold lectures; do experiments; or share data. Currently, there are several virtual worlds, such as Second Life, Whyville, There, and Activeworlds where diverse groups of people interact regardless of age, gender, and ethnicity.

However, activities in virtual worlds, as in any other online environment, can be associated with risks and uncertainties. Gartner (2007a, b) lists the following issues facing institutions in dealing with virtual worlds: information technology risks, identity and access management concerns, loss of confidentiality, brand and reputation damage, and productivity reduction. The European Network and Information Security Agency (ENISA 2010) provided fourteen categories of risks associated with virtual worlds: (1) Avatar identity theft and identity fraud (e.g., theft of account credentials), (2) Massively multiplayer online privacy risks (e.g., disclose more personal data because a false sense of security), (3) Automation attacks (e.g., attackers obtain objects or services for free), (4) Cheating (e.g., illegal object duplication and insider trading), (5) Harassment (ganking and verbal harassment), (6) Trading and financial attacks (e.g. credit card chargebacks), (7) Intellectual property risks (e.g. import copyrighted material without the permission, (8) Risks for minors (e.g., failure of age-verification techniques), (9) Problems with online dispute resolution (e.g., gain advantage over other players or residents), (10) spam (e.g. unsolicited marketing), (11) Denial of service attacks (network resource unavailable (e.g., scripted objects and avatar action make the virtual world unavailable), (12) Malicious game servers (e.g., virtual mugging caused by a malicious game server software), (13) Attacks on user's machine through game client (e.g., a piece of network software allows an attacker to control a user's machine), (14) Access and authorization problems (e.g., avatars collude to physically block other avatars).

Applying economic analysis, Arakji and Lang (2007) explained eight categories of risk associated with firm-based and social production models in virtual worlds: (1) Investment risk (e.g., investors finance a virtual world enterprise, assuming proprietary ownership of intellectual property), (2) Development risk (e.g., the substantial time and cost to develop a complex virtual world contributes to the fixed costs for developing a new product), (3) Coordination risk (e.g., very high coordination costs), (4) Motivation risk (e.g., focusing on extrinsic motivation, and ignoring intrinsic motivation), (5) Control risk (emphasizing product certainty and well-defined virtual world scripts, and ignoring diversity of ideas and support organic, nonlinear game evolution), (6) Security risk (e.g., data security and

business confidentiality concerns), (7) Governance risk (e.g., disagreement on actions and behaviors in massively multiplayer game environments), (8) Culture risk (difference between organizational culture and user community culture).

In spite of the growing popularity of virtual worlds among students, educators have been slow to embrace them in their classrooms (Kirschner and Selinger 2003). One of the reasons for the slow adoption in the classroom has been educators' concern regarding safety risks involved in the virtual environment (Kluge and Riley 2008). But, how do educators understand these risks? Answering this question is essential in using and adapting virtual worlds as a learning technology. Specifically, in this research, we were interested in identifying why educators are apprehensive of virtual worlds. Our research questions were:

1. What are the perceptions of educators regarding risk and uncertainties in virtual worlds, and how do these concerns differ by the level of use of virtual worlds?
2. What behaviors are educators likely to experience in virtual worlds, and how do these behaviors differ by the level of use of virtual worlds?

In this paper, after presenting some background, we discuss the results of a survey, containing multiple-choice and open-ended questions to assess educators' perceptions of risks in virtual worlds and behaviors experienced by them. Then, we briefly present the seminal risk perception model developed by Fischhoff and his colleagues (Fischhoff et al. 1978), our revision to this model, and how these models can help with assessing risks in virtual worlds. Finally, we discuss the implications of our findings for education management.

## Background

### Virtual worlds in education

Virtual worlds have the potential to play an important role in the classroom and educational setting, as they are experiential exercises that transport learners to another world. There they apply their knowledge, skills, and strategies in the execution of their assigned roles (Gredler 2003). For example, educators can use a virtual world, such as Second Life to allow students to experience how various aspects of a system work, such as the economy. Virtual worlds also can engage students in "higher level cognitive thinking, such as interpreting, analyzing, discovering, evaluating, acting, and problem solving" (Antonacci et al. 2008).

Slator et al. (1999) discussed a number of virtual environments for education in various disciplines—ranging from earth science to anthropology and from business to biology. For example, they described Geology Explorer, an online virtual world where students work as geologists to explore geology of a hypothetical planet. The authors also discussed Virtual Cell, which promotes deductive reasoning and problem solving through a bio-environment. The authors argued that virtual environments allow students to assume specific roles in a given context, which provides the aforementioned authentic and meaningful learning experience; hence they learn by doing rather than being passive participants in their learning. In

addition, students can learn in virtual worlds because they provide action possibilities not available through traditional means by creating shared spaces and experiences for participants in different physical locations (Slator et al. 1999). Kluge and Riley (2008) further argued that virtual worlds allow instructors to change their teaching from teacher-directed to student-centered as students actively engage in creating, discussing, and interacting with tools in an authentic context that resembles real-world situations. Students learn in a virtual world through role-playing, operating simulated equipment, designing and building things, or interacting with simulations (Antonacci et al. 2008). These activities engage "students in higher-level cognitive thinking, such as interpreting, analyzing, discovering, evaluating, acting and problem solving". Virtual worlds can also play an important role in distance education by allowing students to communicate and "hang-out" in a common place. Dickey (2005) found that virtual environments allow learners in distance courses "to converse and construct in a collaborative environment because of the types of design features it affords." These features include unique names and avatars, which provide trust and accountability while also allowing students to adopt new roles that are available in traditional learning environments.

However, in spite of the numerous advantages virtual worlds have to offer, several challenges remain for implementing virtual worlds in the classroom. Some of these challenges include: highly technical requirements for computer systems; a steep learning curve to control avatars; potential for harassment, humiliation, victimization, or other distractions; and lack of environmental control unless situated in a private area (Harris and Rea 2009). In addition, users of virtual worlds have concerns regarding privacy, anonymity and security within the virtual world. However, there is limited research on whether educators and students have similar concerns about the role of virtual worlds in their own classroom. Hence, it is important to understand what challenges exist for educators in implementing these technologies in their classroom.

## Risks and uncertainties in virtual worlds

Knight (1921) made his famous distinction between risk and uncertainty by explaining that risk is ordinarily used in a loose way to refer to any sort of uncertainty viewed from the standpoint of an unfavorable contingency, and uncertainty similarly with reference to favorable outcomes. Understanding and measuring risk enables people to choose prudent courses of action and make appropriate investments in protection and mitigation. For the purpose of this paper, we adapt Knight's definition of risk and uncertainty.

Virtual worlds are commonly perceived as being completely separate from the real lives of their users and therefore immune to the privacy risks and uncertainties posed by other emerging platforms such as social networks (ENISA 2010). However, representing a user as an avatar is not that different from any other form of online persona—users are free to present as accurate or inaccurate a picture as they choose. This may expose virtual world users to many kinds of privacy risks, (e.g., identity disclosure). Certain characteristics of the avatar owner can be guessed

with reasonable accuracy based on statistical analysis. For example, a survey of the 2001 fantasy game Everquest, with 889 users, showed that only 2.5 % of female users and 15.7 % of male users had played characters of the opposite gender. Thus, using these figures, if an avatar in this game is male, his owner is very likely to be male (84.3 % of males and 2.5 % of females will play a male character, and male gamers generally vastly outnumber females) (Yee 2001). According to ENISA (2010) many service providers implement extensive mining features within their gaming environment to detect anomalous and harmful game-play.

Security in virtual worlds may refer to many aspects of protecting a system from unauthorized use (e.g., authentication of users). For this paper, we will limit our treatment of security to the concepts associated with how well a system protects access to information it contains. The concept of privacy goes beyond security and examines how well the use of information conforms to the explicit or implicit assumptions regarding that use. There is an important distinction that we recognize when discussing privacy from a virtual worldview. From an end user perspective, privacy can be considered as preventing storage of personal information, or it can be viewed as ensuring appropriate use of personal information (Karat et al. 2009). For the purposes of this paper, a simple but useful definition of privacy is: The ability of virtual world users to control the terms under which their personal information is acquired and used.

Anwar and Greer (2011) explained the need for privacy and trust in popular learning activities such as peer-tutoring, peer-reviewing, learning object selection, collaboration, group learning, evaluation, role-playing, and personalization. While each of these activities is an instance where trust is needed in an e-learning environment, we want to point out that the absence of trust requires that the learner(s) focus her/his cognitive efforts on negotiating trust instead of on learning. Vandalism in virtual worlds may involve damaging virtual property and real estate, such as defacing buildings, placing obscene structures in public places, etc. (Elliott 2008; Lee 2009). For example, Second Life Liberation Army (SLLA), a radical, anti-corporate organization has performed acts of vandalism in the virtual world on corporate storefronts, such as American Apparel and Reebok, in an effort to promote its cause (Bray and Konsynsky 2007). Vandalism in virtual worlds might make the citizens feel "unsafe" and the cyberworld itself as a "scary" place similar to negative outcomes associated with vandalism in offline public places (Williams 2004).

In addition to many security and privacy issues, virtual world users are exposed to safety issues such as cyberbullying and cyberstalking. Cyber-bullying can be defined as an "aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself" (Smith et al. 2006). Cyberstalking is defined as "the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals."(D'Ovidio and Doyle 2003). Research on prevalence of cyberbullying has suggested that percentage of students who report being cyberbullied has ranged from 7 to 35 % while percentage of students that engage in cyberbullying ranges from 12 to 28 % (Holfeld and Grabe 2012). There also seems to considerable

overlap between traditional bullying and cyber forms of bullying. For example, (Hinduja and Patchin 2008) reported that "youth who reported bullying others in real life in the previous six months were more than 2.5 times as likely to report bullying others on-line. Similarly, youth who were victims of traditional bullying in the previous 6 months were more than 2.5 times as likely to be victims of cyberbullying". Previous research has also suggested that cyberbullying is related to age with older students more likely to engage in cyberbullying than younger students (Cross et al. 2009).

### Using risk perception models

Seminal research by Fischhoff and his colleagues (Fischhoff et al. 1978) investigated perceptions of technology risks, and particularly ways to determine when a product is perceived acceptably safe by laypeople. Their nine constructs of risks can be adopted and used to define risk perceived by the educators who use virtual worlds:

1. Voluntariness—Does the educator voluntarily get involved in the virtual world?
2. Immediacy of effect—To what extent is the risk of consequence from the educator's actions immediate?
3. Knowledge about risk—To what extent are the risks known (precisely) by the educator who is exposed to those risks?
4. Knowledge of science—To what extent are the risks precisely known and quantified?
5. Control over risk—To what extent can the educator, by personal skill or diligence, avoid the consequences to him/her while engaging in untoward activity?
6. Chronic or catastrophic—Does the risk affect the educator over time, or is it a risk that affects a larger number of people at once?
7. Newness—Are these risks new to the educator or is there some prior experience/conditioning?
8. Common dread—Is this a risk that the educator has rationalized and can think about reasonably calmly?
9. Severity of consequences—When is the risk from the activity realized in the form of consequences to the educator?

In our previous research, we have developed an approximation model—based on the psychometric model of risk perception developed by Fischhoff and his colleagues—in which characteristics of a risk are correlated with its acceptance (Farahmand et al. 2008). We successfully used this model in several real-world studies, for example, in describing the risk-taking behavior of insiders. We validated our findings with forty-two senior information security executives from a variety of organizations across the US. For more information see Farahmand and Spafford (2013).

In our model, we consider risks that are undertaken voluntarily are generally considered more acceptable than risks imposed without consent. Similarly, risks that cause dreaded forms of harm are also considered to be less acceptable. We

condensed Fischhoff's nine variables of risk–voluntariness, immediacy of effect, knowledge about the risk (known by the person), knowledge about the risk (known to science), control over the risk, novelty, chronic or catastrophic, degree of dread, severity of consequences–by considering *understanding* (familiarity and experience) and *consequences* (scope, duration, and impact) as the two principal characteristics of information security and privacy risks. For more information about this model and its real world application see Farahmand and Spafford (2013).

## Method

### Participants

Seventy-seven participants completed the survey. Of these participants, 77 % were older than 35, and 79 % were male. Eighty-three percent of participants worked at the colleges of liberal arts in academic institutions, while the remaining reported working at "other" places of employment, such as industry, non-profit organizations, etc.

### Survey instrument

In this paper to understand the significance of security, privacy, and safety risks and uncertainties in virtual worlds—while being used as a learning technology—we developed a survey to investigate how educators perceive these risks and how their level of use of virtual worlds influences their risk perception level.

Questions regarding the use of virtual environments in daily life were adapted from the teens' use of media reported by the Pew Internet and American Life Project (Lenhart et al. 2007). The work of Hinduja and Patchin (2008) influenced the questions in regards to experienced behavior in virtual environments such as cyber bullying, cyber-staking, flame discussions, etc. Questions on the assessment of risks and uncertainties were developed during the first stage of this research project, revised for virtual worlds, and validated with end users. Finally, questions on the governance and regulations of virtual environments were derived from the work of Balkin and Noveck (2006). In addition to four demographic questions, survey contained 15 questions to gauge participants' frequency of use of virtual worlds, their risk perception of the virtual world, and behaviors experienced in the virtual world. Internal reliability of the survey was calculated using Cronbach's alpha (0.823), which was deemed sufficient.

### Procedure

Because our target population was the educational sector, the survey was distributed to several different mailing lists including organizations such as Educause, the Association for Educational Communication and Technology (AECT), Association for the Advancement of Computers in Education (AACE), the Association of Internet Researchers (AoIR), several high traffic email lists for technology

coordinators and computer teachers in K-12 schools, and specialized lists for computer security. The email contained a link to the online survey, which was hosted by Qualtrics, an online survey service. Participants could click on the link and complete the survey at their convenience. The survey, however, did not allow participants to save their responses and complete the survey at a later time; hence, they had to complete the survey all at once. The survey contained multiple-choice questions (one answer or more than one answer) and open-ended questions, in which participants were encouraged to provide a full answer using their knowledge and/or feelings. The survey was open for a period of three months.

### Data analysis

In this survey, we sought answers to the research questions about educators' perceptions of security, privacy, and safety risks involved with virtual worlds. The following section discusses the results of the survey. Specifically, participants who reported using a virtual world once a week were classified as infrequent users, participants who logged into a virtual world a few times a week were considered to be normal users, and those who logged on everyday/multiple times a week were classified as frequent users. The data then was analyzed using descriptive statistics and frequency analysis. We also analyzed participants' concerns with virtual worlds and behaviors experienced in virtual worlds based upon their level of use of virtual worlds. We conducted a Multivariate Analysis of Variance (MANOVA) to examine differences between the level of use and participants' concerns and behaviors experienced in the virtual worlds. We also followed up the MANOVA analysis with a univariate analysis (ANOVA).

## Results

### Concerns with virtual world

The results discussed in this section address the first research question regarding perceptions of educators regarding security, privacy, and safety of virtual worlds. Results suggested that overall; participants were concerned about the virtual worlds. Specifically, 47 % of participants expressed high concern with regards to intrusion risk, and 38 % of the participants had low to middle level concern about this category of risks. The majority of the participants (53 %) were highly concerned about confidentiality issues with regards to what they say might be recorded or stored. More participants (40 %) also reported being concerned about identity issues and not being able to identify who was behind an avatar, whereas 34 % had low or no concern about it. The impact of virtual worlds on participants' productivity and reputation were also concerns for more participants, even though only slightly (36 vs. 32 %). Figure 1 presents these results graphically.

The results discussed above present a snapshot of all the participants; however, we wanted to further examine how the level of use of virtual worlds influences participants' concerns.

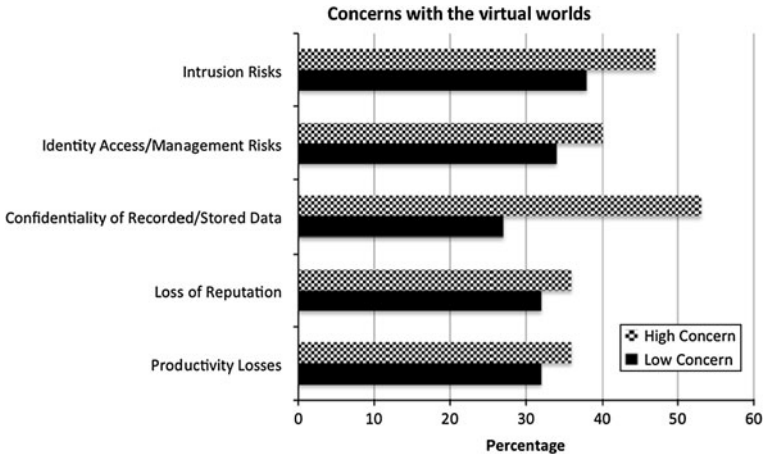


**Fig. 1** Concerns with virtual worlds (Note: numbers do not add to 100 % because some participants were neutral towards these concerns)

The results suggested that normal users, who were 55 % of our total participants, are less likely to feel safe when compared to infrequent and frequent users. Specifically, normal user had higher concerns about the virtual world compared to infrequent and frequent users. Normal users reported having very high concerns about the virtual environment in terms of the intrusion risks, identity access/management risks, confidentiality of recorded/stored data, loss of reputation, and productively losses. It is interesting to note that both infrequent and frequent users had less concerns about these issues across the board where frequent users were least concerned about these issues. Figure 2 below shows this graphically.

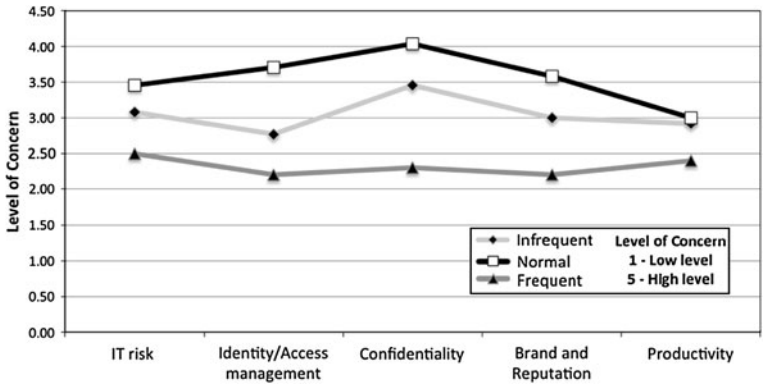


**Fig. 2** Concerns with the virtual world based on level of use (Note: the *numbers* represent means for the level of user)

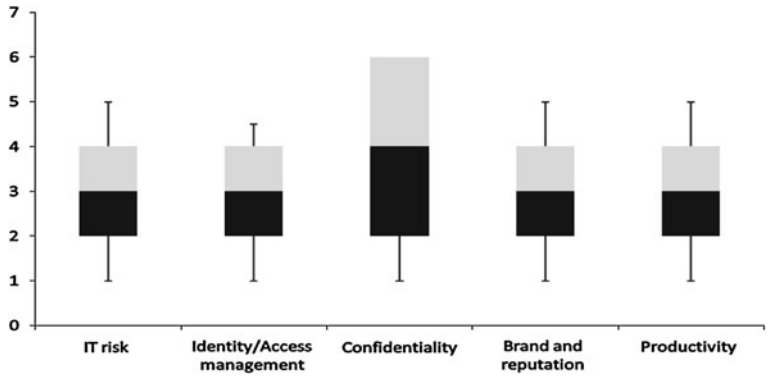


**Fig. 3** *Boxplot* of concerns with virtual worlds.The *bottom black cap* represents the minimum value. The *bottom box* boundary represents the 25th percentile or *lower* fourth. The *box* divider represents the median. The *top box* boundary represents the 75th percentile or *upper* fourth. The topmost *black cap* represents the maximum value

Figure 3 shows the boxplots of concerns with virtual worlds. The range for IT risks, confidentiality, brand and reputation was 5, while identity/access management and productivity had a range of 5. Across the different level of users, infrequent users had a range of 4 for all the items relating to concerns with virtual worlds except for productivity, which had a range of 5. Normal users had a range of 5 for productivity, range of 4 for IT risks and brand and reputation, a range of 3 for identity/access management and confidentiality. Frequent users had a range of 5 for productivity, range of 4 for IT risks, identity/access management and confidentiality, a range of 3 for brand and reputation.

MANOVA results suggested that there was a significant main effect for the concerns about virtual worlds by the level of use, $F(5, 41) = 2.73$, $p = 0.03$, $\eta_p^2 = 0.25$, $1 - \beta = 0.76$. Follow-up ANOVA analysis suggested that there was a significant difference between level of users for Identity/Access Management [$F(2,44) = 5.12$, $p = 0.01$, $\eta_p^2 = 0.19$, $1 - \beta = 0.80$], Confidentiality [$F(2,44) = 6.71$, $p = 0.00$. $\eta_p^2 = 0.23$, $1 - \beta = 0.90$, and Brand and Reputation [$F(2,44) = 4.64$, $p = 0.01$, $\eta_p^2 = 0.17$, $1 - \beta = 0.77$]. There were no significant differences between the users for IT Risk [$F(2, 44) = 2.03$, $p = 0.14$, $\eta_p^2 = 0.08$, $1 - \beta = 0.40$], and Productivity [$F(2,44) = 0.56$, $P = 0.57$, $\eta_p^2 = 0.03$, $1 - \beta = 0.14$]. A pairwise comparison analysis revealed that normal users were more significantly concerned than frequent users ($p = 0.014$) about not being able to verify who was behind an avatar in a virtual world (identity/access management). Results also indicated that normal users were significantly more concerned about confidentiality ($p = 0.002$) and brand/reputation ($p = 0.013$) than frequent users. See Tables 1 and 2 for descriptive and inferential statistics.

**Table 1** Means and standard deviation for the concerns about virtual worlds

| | IT risk Mean (SD) | Identity management Mean (SD) | Confidentiality Mean (SD) | Brand and reputation Mean (SD) | Productivity Mean (SD) |
|---|---|---|---|---|---|
| Infrequent | 3.08 (1.32) | 2.77 (1.48) | 3.46 (1.26) | 3.00 (1.22) | 2.92 (1.44) |
| Normal | 3.46 (1.10) | 3.71 (1.23) | 4.04 (1.12) | 3.58 (1.25) | 3.00 (1.50) |
| Frequent | 2.50 (1.58) | 2.20 (1.40) | 2.30 (1.57) | 2.20 (1.14) | 2.40 (1.71) |

**Table 2** Results of MANOVA and ANOVA for the concerns about virtual worlds

| Dependent variable | *df* | F-statistics | *p* value | Partial eta squared | Power |
|---|---|---|---|---|---|
| Level of use[a]* | 5, 41 | 2.73 | 0.032 | 0.25 | 0.76 |
| IT risk | 2, 44 | 2.03 | 0.14 | 0.08 | 0.40 |
| Identity/access management* | 2, 44 | 5.12 | 0.01 | 0.19 | 0.80 |
| Confidentiality* | 2, 44 | 6.71 | 0.00 | 0.23 | 0.90 |
| Brand and reputation* | 2, 44 | 4.64 | 0.01 | 0.17 | 0.75 |
| Productivity | 2, 44 | 0.56 | 0.57 | 0.03 | 0.14 |

* Significant values

[a] MANOVA statistics; other statistics are from ANOVA

## Behaviors experienced in virtual worlds

The results discussed in this section address the second research question regarding behaviors experienced by educators in the virtual worlds. Participants were also asked about the types of behaviors they experienced in the virtual worlds. Overall, results suggest that participants rarely experienced any threatening behavior in virtual world. For example, 68 % of the participants reported they rarely experienced cyber bullying and only 17 % reported frequently experiencing cyber-bullying. Similarly, only seven percent frequently encountered virtual stalking while 77 % faced virtual stalking. When asked about being involved in a heavy argument in a virtual world, 23 % reported that they experienced it frequently while 60 % rarely came cross it. Twenty three percent of participants also revealed encountering vandalism in a virtual world while 74 % rarely faced it. Finally, 81 % of the participants reported rarely having their artifact/code stolen and 11 % had frequently experienced theft of artifacts/code. Figure 4 presents these results graphically.

We also analyzed the data on behaviors experienced based on level of participants' use of virtual worlds. When asked about what types of behaviors participants has experienced in a virtual world, results were more scattered based on level of use. When participants were asked about how frequently they experienced cyber-bullying, frequent users reported to having experienced it more that infrequent and normal users. Frequent users also reported being involved in a heavy argument (flame) in a virtual environment as compared to infrequent and

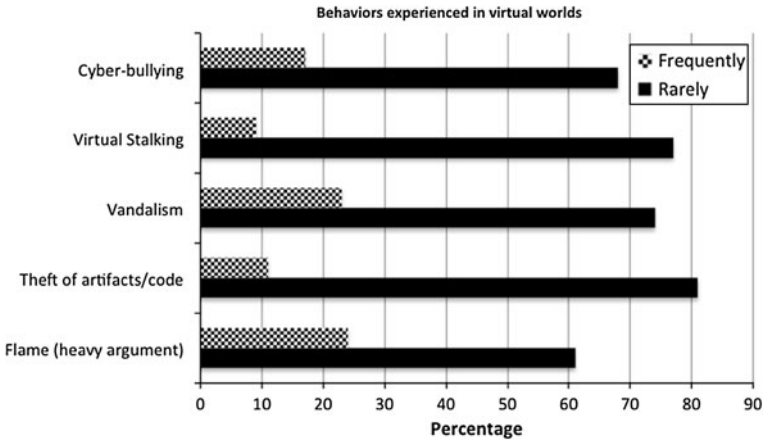


**Fig. 4** Behaviors experienced in virtual worlds (Note: numbers do not add to 100 % because some participants were neutral towards these concerns)

normal users. Normal users reported having experienced the least flame (heavy argument). When asked about theft of artifacts/code infrequent users reported having experienced it more than normal and frequent users. Infrequent users also experienced virtual stalking slightly more than frequent and normal users, who experienced it the least. In terms of experiencing vandalism in virtual environment, frequent users reported experiencing it slightly more than normal and infrequent users (see Fig. 5).

Figure 6 shows the boxplots of behaviors experienced in virtual worlds. The range for cyber bullying, virtual stalking, vandalism, theft of artifact/code, and flame was 4. Across the different level of users, infrequent users and normal users had a range of 4 for all the behaviors experienced in the virtual world. Frequent users had a range of 3 for cyber bullying, virtual stalking, and vandalism, range of 2 for theft of artifact/code, and a range of 4 for flame (see Fig. 6).

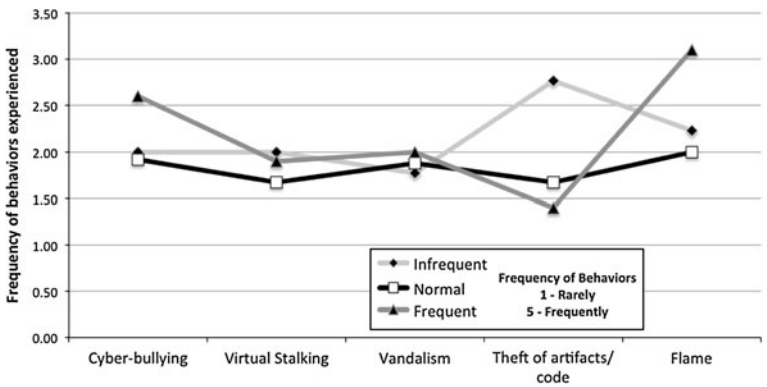


**Fig. 5** Behaviors experienced in the virtual world based on level of use (Note: the *numbers* represent means for the level of user)

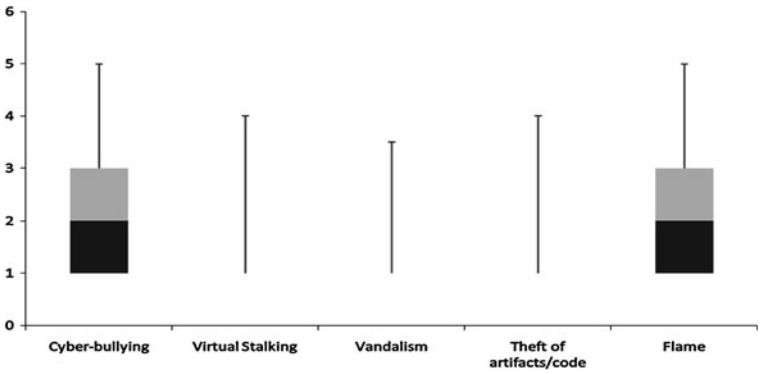


**Fig. 6** *Boxplot* of behaviors experienced in virtual world. The *bottom black cap* represents the minimum value. The *bottom box* boundary represents the 25th percentile or *lower* fourth. The *box* divider represents the median. The *top box* boundary represents the 75th percentile or *upper* fourth. The topmost *black cap* represents the maximum value

Fifty four percent of the participants reported an increase in these behaviors while 48 % reported a decrease in such behaviors. However, a majority of the participants did not feel threatened as an avatar (68 %) or as a person acting in a virtual world (83 %). It is interesting to note that more people felt threatened as an avatar than as acting as a person.

MANOVA results suggested that there was a significant main effect for behaviors experienced in the virtual workds by the level of use, $F(5, 40) = 2.59$, $p = 0.04$, $\eta_p^2 = 0.25$, $1 - \beta = 0.74$. However, follow-up ANOVA results showed no significant differences for any of the dependent variables, cyber-bullying [$F(2,43) = 1.34$, $p = 0.27$, $\eta_p^2 = 0.06$, $1 - \beta = 0.27$], virtual stalking [$F(2,43) = 0.52$, $p = 0.60$, $\eta_p^2 = 0.02$, $1 - \beta = 0.13$], vandalism [$F(2,43) = 0.10$, $p = 0.91$, $\eta_p^2 = 0.00$, $1 - \beta = 0.06$], theft of artifact [$F(2,43) = 0.31, p = 0.73, \eta_p^2 = 0.01, 1 - \beta = 0.10$], and flame [$F(2,43) = 2.20, p = 0.12, \eta_p^2 = 0.09, 1 - \beta = 0.43$]. See Tables 3 and 4 for descriptive and inferential statistics may be partially explained by this research.

Finally, a correlation was computed to assess the relationship between participants' risk perception of the virtual world and the behavior experienced in the virtual world. Each participant received a total risk perception score and a total behavior experience score. Results suggested that the two variables were not significantly correlated, $r = 0.19$, $p = 0.20$ (see Fig. 7).

**Tables 3** Means and standard deviation for behaviors experienced in virtual worlds

| | Cyber-bullying Mean (SD) | Virtual stalking Mean (SD) | Vandalism Mean (SD) | Theft of artifact Mean (SD) | Flame Mean (SD) |
|---|---|---|---|---|---|
| Infrequent | 2.00 (1.35) | 2.00 (1.53) | 1.77 (1.54) | 1.77 (1.36) | 2.23 (1.42) |
| Normal | 1.83 (1.30) | 1.61 (1.03) | 1.78 (1.35) | 1.57 (1.08) | 2.00 (1.41) |
| Frequent | 2.60 (0.97) | 1.90 (0.99) | 2.00 (1.41) | 1.40 (0.84) | 3.10 (1.29) |

**Table 4** Results of MANOVA and ANOVA for the behaviors experienced in virtual worlds

| Dependent variable | *df* | F-statistics | *p* value | Partial eta squared | Power |
|---|---|---|---|---|---|
| Level of use[a] | 5, 40 | 2.59 | 0.04 | 0.25 | 0.74 |
| Cyber-bullying | 2, 43 | 1.34 | 0.27 | 0.06 | 0.27 |
| Virtual stalking | 2, 43 | 0.52 | 0.60 | 0.02 | 0.13 |
| Vandalism | 2, 43 | 0.10 | 0.91 | 0.00 | 0.06 |
| Theft of arifact | 2, 43 | 0.31 | 0.73 | 0.01 | 0.10 |
| Flame | 2, 43 | 2.20 | 0.12 | 0.09 | 0.43 |

[a] Indicates MANOVA statistics; other statistics are from ANOVA

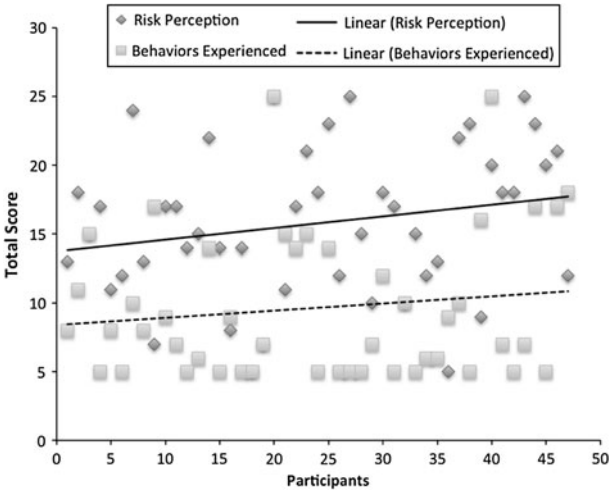


**Fig. 7** Risk perception versus behavior in virtual world

## Discussion

This research sheds light on perceptions of educators regarding risk and uncertainties in virtual worlds, how these concerns differ by the level of use of virtual worlds, and the behaviors they actually experienced in virtual worlds. Our results reveal a divergence between risk perception and reality in virtual worlds. This finding is an important issue in using virtual worlds as a learning technology that needs to be well understood. We use a commonly accepted risk perception model developed by Fischhoff and his colleagues and our revision to this model to explain this divergence. Our research also has several implications for education management. These can be summarized as follows.

### The divergence between risk perception and reality in virtual worlds

The results of our study indicate a divergence between perception of risks and their actual experience in virtual worlds (see Fig. 7). Overall, results suggested that

normal users are less likely to feel safe, compared to infrequent and frequent users (see Fig. 2). The multivariate tests suggested that the level of participants' use of virtual world had a significant effect on their overall safety concerns about the virtual worlds. Follow-up univariate test suggest that there were significant differences among the levels of users (frequent, normal, and infrequent) about their safety concerns. In particular, normal users were significantly more concerned about identifying who was behind an avatar, confidentiality of their stored data on servers, and loss of reputation by one's own actions or actions of others in the virtual world. There were no differences between level of use and participants' concerns about loss of productivity and that virtual world client might allow intrusion on their computers. The multivariate tests also suggested significant effect on behaviors' experienced in virtual worlds based upon participants' level of use of virtual world. However, follow-up univariate analysis did not find any significant differences among the groups on cyber-bullying, virtual stalking, vandalism, theft of artifact, or flame (heavy argument).

Our contraposed findings could be partially explained by the findings of Slovic and Peters (2006). Educators perceive and act on risk in two fundamental ways: (a) Risk as feelings which refers to their instinctive and intuitive reactions to risks and uncertainties, (b) risk as analysis which refers to logic, reason, and scientific deliberation to bear on risk management. The divergence between the risk perceived by educators and the reality in the virtual worlds (i.e., difference between perception of risks and their actual experience in virtual worlds, as shown in Fig. 7) indicates that educators are more likely to perceive and act on risks in virtual worlds based on their feelings of risk than based on actual risk analysis.

Even though some of the results are not significant, it is interesting to note that there are some differences between the groups as a result of their frequency of use of the virtual worlds. For example, normal users were more concerned about identity management, confidentiality, and reputation than frequent and infrequent users. However, when participants were asked about how frequently they actually experienced different incidents (e.g., cyber-bullying, virtual stalking, etc.) frequent users reported to having experienced it slightly more than infrequent and normal users (see Fig. 5). Why is this so? To understand these results, we turn to the work of seminal researchers in the field. Schneier (2008) argued, "Security is both a feeling and a reality. The reality of security is mathematical, based on the probability of different risks and the effectiveness of different countermeasures. But security is also a feeling, based not on probabilities and mathematical calculations, but on our psychological reactions to both risks and countermeasures, and the first, and most common area that can cause the feeling of security to diverge from the reality of security is the perception of risk." A dual process approach to risks is not limited to information privacy and security risks and in virtual worlds (Camerer et al. 2005).

Our approximation model—based on the psychometric model of risk perception developed by Fischhoff and his colleagues (Fischhoff et al. 1978)–that was explained in the background section of this article, can also be used to explain the results of our study. The perceived risk by educators is a function of consequence and understanding. An approximate perceived risk score may be constructed from the consequence metric and the inverse of the understanding metric. The perceived

risk score therefore increases whenever the consequences are more severe for educators, and decreases as the educator gains deeper understanding of the nature and limits of the risk. Considering that the participants in our study were not security experts (83 % of participants in our study worked at the colleges of liberal art in academic institutions), they did not have a deep understanding of the technical risks in virtual worlds. Therefore, they perceived more risks to be associated with the virtual worlds.

## Implications for education management and future research

Making decisions about using virtual worlds as learning technologies without consideration of perception of risk is not likely to be optimal. Given that virtual worlds allow for a strong social network, where students can communicate, participate in groups, publicize events, etc., it is imperative that they feel safe.

Educators should consider user perceptions of risk when establishing trust with their in-world participants, i.e., students. As Anwar and Greer (2011) argued: "Privacy and trust are equally desirable in a learning environment. Privacy promotes safe learning, while trust promotes collaboration and healthy competition, and thereby, knowledge dissemination." To address this, educational policies should be aligned with perceptions. Efforts should be made to develop a standardized approach to trust and risk across different communities to reduce the burden on participants who seek to better understand and comply with policies and practices of the particular virtual world. Individual participants expect a given educational activity in which they engage to be conducted fairly and address their privacy concerns. By ensuring this fairness and respecting privacy concerns, educators give their participants the confidence to disclose or reveal personal information—and to allow that information subsequently to be used to create effective profiles for real-world use.

Fishhoff (2006) argued that effective risk communication can fulfill parts of the social contract between those who create risks (as a byproduct of other activities) and those who bear them (perhaps along with the benefits of those activities). To have an effective risk communication in virtual worlds, we recommend that educators:

- Determine the facts central to the decisions that all participants face,
- Determine what students know already about security, privacy, and safety,
- Design messages closing the critical gaps-repeating until an acceptable level of understanding has been achieved,
- Let students know that this is a safe environment where participants are treated respectfully.

Our study indicates that the mechanisms for understanding risk perception by virtual world participants may need to take into account the knowledge of the hazards as to the possible extent of consequences, and be measured over a time interval rather than at some specific instant. This approach will lead to more robust models and evaluations, and thus result in better policies for governance in virtual worlds.

Finally, educators also face the challenges of cyber-bullying in virtual worlds. Given that cyber-bullying has the same impact as traditional bullying (Anwar and Greer 2011) it is imperative for educators to discuss the risk and security of virtual world with students.

Future research needs to develop a classification of hazards—caused by security and privacy incidents—that can be used to understand and to predict educational institution responses to perceived risks. Such a scheme might explain, for example, educational communities' extreme aversion to hazards of some privacy and security incidents, their indifference to others, and discrepancies among different organizational opinions.

In this paper, we offer a starting point for profiling and measuring perceived risk to guide institutions in developing their risk management plan in employment of virtual world environments to serve education and training. Further investigation is required to present a comprehensive measure for policies in security risk management. The implications extend well beyond the microcosm of the education and training environments. Collaboration with experts from different academic disciplines, government, and industry is required for the success of such an investigation.

**Acknowledgments** Portions of this work were supported by the National Science Foundation under Grant No. 1230507, and CERIAS at Purdue University. The authors wish to thank Dr. Johannes Strobel for his contribution to survey development and distribution, and Dr. Melissa Dark for her comments.

## References

Antonacci, D., DiBartolo, E. N., Fritsch, K., McMullen, B., & Murch-Shafer, R. (2008). The power of virtual worlds in education: A second life primer and resource for exploring the potential of virtual worlds to impact teaching and learning. Angel Learning.

Anwar, M., & Greer, J. (2011). Facilitating Trust in Privacy-preserving E-learning Environments. *IEEE Transactions on Learning Technologies*, published online = .

Arakji, R. Y., & Lang, K. R. (2007). The virtual cathedral and the virtual bazaar. *The Database for Advances in Information Systems, 38*(4), 33–39.

Balkin, J., & Noveck, B. (2006). *State of play: Law, games, and virtual worlds*. New York, NY: NYU Press.

Bray, D. A., & Konsynsky, B. R. (2007). Virtual worlds: Multi-disciplinary research opportunities. *The Data Base for Advances in Information Systems, 38*(4), 17–25.

Camerer, C., Lowestien, G., & Prelec, D. (2005). Neuroeconomics: How neuroscience can inform economics. *Journal of Economic Literature*, Vol. XLIII 9–64.

Cross, D., Shaw, T., Hearn, L., Epstein, M., Monks, H., Lester, L., et al. (2009). *Australian covert bullying prevalence study (ACBPS)*. Perth: Child Health Promotion Research Centre, Edith Cowan University.

D'Ovidio, R., & Doyle, J. (2003). A study on cyberstalking understanding investigative hurdles. *Law Enforcement Bulletin, 72*(3), 10–21.

Dickey, M. D. (2005). Three-dimensional virtual worlds and distance learning: Two case studies of active worlds as a medium for distance education. *British Journal of Educational Technology, 36*(3), 439–451.

Elliott, J. (2008). Help—somebody robbed my second life avatar. *Journal of Virtual Worlds Research, 1*(1), 1–11.

ENISA (2010). Virtual worlds, real money; Security and Privacy in massively-multiplayer online games and social and corporate virtual worlds. European network and information security agency.

Farahmand, F., Atallah, M., & Konsysnski, B. (2008). Incentives and Perceptions of Information Security Risks. *Twenty Ninth International Conference on Information Systems*, ICIS 2008, Paris, p. 16.

Farahmand, F., & Spafford, E. H. (2013) Understanding insiders: An analysis of risk- taking behavior. *Information Systems Frontiers*, Springer Publications, pp. 11, to appear.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Science, 9*(2), 127–152.
Fishhoff, B. (2006). The psychological perception of risk. *The McGraw-Hill Homeland Security Hanbook*, pp. 463–493.
Gartner (2007a). *Corporate use of virtual worlds needs careful evaluation*. Gartner Group, Retrieved from http://www.gartner.com/it/page.jsp?id=511370.
Gartner (2007b). *Five virtual world security fears*. Retrieved from http://www.businessweek.com/globalbiz/content/aug2007/gb2007089_070863.htm?chan=globalbiz_europe+index+page_top+stories.
Gartner (2009). "Gartner Says 80 Percent of Active Internet Users Will Have A "Second Life" in the Virtual World by the End of 2011," Gartner Group, Retrieved from http://www.gartner.com/it/page.jsp?id=503861.
Gredler, M. E. (2003). Games and simulations and their relationships to learning. *Handbook of research for educational communications and technology* (2nd ed., pp. 571–581). Mahwah, NJ: Lawrence Erlbaum Associates.
Harris, A. L. & Rea, A. (2009). Web 2.0 and virtual world technologies: A growing impact on IS Education. *Journal of Information Systems Education, 20*(2), 137–144.
Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29*(2), 1–29, 129–156.
Holfeld, B., & Grabe, M. (2012). An examination of the history, prevalence, characteristics, and reporting of cyberbullying in the United States. In Q. Li, D. Cross, & P. K. Smith (Eds.), *Cyberbullying in the global playground: Research from international perspectives* (pp. 117–142). Malden, MA: Wiley-Blackwell.
Karat, J., Karat, C. M., Bertino, E., Li, N., Ni, Q., Brodie, C., et al. (2009). A policy framework for security and privacy management. *IBM Journal of Research and Development, 53*(2), 242–255.
Kirschner, P., & Selinger, M. (2003). The state of affairs of teacher education with respect to information and communications technology. *Technology, Pedagogy and Education, 12*(1), 5–12.
Kluge, S., & Riley, L. (2008). Teaching in virtual worlds: Opportunities and challenges. *Issues in Informing Science and Information Technology, 5*, 127–135.
Knight, F. H. (1921). *Risk, uncertainty and profit*. Gloucester, UK: Dodo press.
Lee, C. Y. (2009). Understanding security threats in virtual worlds. In *Proceedings of the fifteenth Americas conference on information systems*. San Francisco, CA: Association for Information Systems.
Lenhart, A., Madden, M., Macgill, A. R., & Smith, A. (2007). Teens and social media. *Pew Internet & American Life Project*.
NSF (2008). *Fostering learning in the networked world: The cyberlearning opportunity and challenge*. Report of the NSF Task Force on Cyberlearning, National Science Foundation, 2008.
Schneier, B. (2008). The psychology of security. http://www.schneier.com/essay-155.html.
Slator, B. M., Juell, P., McClean, P. E., Saini-Eidukatc, B., Schwertc, D. P., Whited, A. R., et al. (1999). Virtual environments for education. *Journal of Network and Computer Applications, 22*, 161–174.
Slovic, P., & Peters, E. (2006). Risk perception and affect. *Current Directions in Psychological Sciences, 15*(6), 322–325.
Smith, P., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. *Research Brief,* Brief No: RBX03-06.
Stross, C. (2007). *Halting state*. New York: Ace Books.
Vinge, V. (1981). *True names.* Retrieved from http://www.facstaff.bucknell.edu/rickard/TRUENAMES.pdf.
Williams, M. (2004) Understanding king punisher and his order: Vandalism in a virtual reality community—motives, meanings and possible solutions. Internet Journal of Criminology.
Yee, N. (2001). Everquest survey. Retrieved from http://www.nickyee.com/eqt/report.html.

## Author Biographies

**Fariborz Farahmand** is a research assistant professor at Purdue University. Dr. Farahmand has received several awards for excellence in scholarship and education, including a fellowship from the Institution for Information Infrastructure Protection (I3P). His research focuses on human centered computing and applications of behavioral economics in security and privacy of information systems, vulnerability and risk assessment of information systems, and technology policy.

**Aman Yadav** is an associate professor at Purdue University. Dr. Yadav has received several awards for excellence in scholarship and education, including Purdue Teaching for Tomorrow Award. His research focuses on problem-based learning and case-based instruction in Science, Technology, Engineering, and Mathematics (STEM) disciplines. He also examines the use of video cases in teacher professional development and the role of epistemological beliefs in preservice teacher education.

**Eugene H. Spafford** is a professor at Purdue University, and is the founder and Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS). His research and education over three decades has contributed to many of the technologies used in modern computing system protection. Spaf's current research interests are in information security, cybercrime, software engineering, professional ethics, and security policy. Dr. Spafford is a Fellow of the ACM, AAAS, IEEE, $ISC^2$, is a Distinguished Fellow of the ISSA, and has received many other awards for service, scholarship, and education.