

The Influence Of Knowing Web 2.0 Risks And Controls On Web 2.0 Usage And Security Practices Of Online Users

Riaan J. Rudman, Stellenbosch University, South Africa

ABSTRACT

Significant changes have taken place on the internet in recent years. The most prominent is the introduction of Web 2.0 technologies (Web 2.0), which promotes sharing and collaboration. This study investigates the usage patterns, and awareness levels of the risks and controls associated with Web 2.0 by educated and uneducated users. Accounting students (as a proxy for educated users) are taught about the risks and controls of Web 2.0 as part of their studies, whereas Business Strategy students' (as a proxy for uneducated users) exposure is limited to popular media and their own research.

The results indicate that the use of Web 2.0 is popular among South African students irrespective of which course they major in. The Web 2.0 awareness levels of both populations were relatively high with no significant differences. Contrary to expectation, the level of usage; types of Web 2.0 technologies; types of risks; and the manner and frequency of sharing of information by the two populations were not found to differ significantly.

The research highlights that although Accounting students are taught about the risks and controls in Web 2.0, they do not take these risks and controls into consideration in their personal life when interacting with Web 2.0. Contrary to expectation, it appears that being formally educated on Web 2.0 does not have a larger impact on user behaviour than awareness gained from popular media. It also indicates how user behaviour influences the effectiveness of online controls.

Keywords: Internet Risks; Web 2.0; Usage Patterns; User Behaviour; Online Controls

1. INTRODUCTION

The manner in which technology is being used is evolving, convergence of technologies is taking place, the level of integration between platforms is increasing, and collaboration has taken prominence (Trevathan & Myers, 2012). Often these developments are driven by Web 2.0 technologies (referred to as 'Web 2.0' hence forth). Although numerous definitions for 'Web 2.0' exist, it is not well defined and is continuously evolving¹. In principle, Web 2.0 is a perceived second generation of web-based communities that facilitate collaboration and sharing between users; referring to a change in the way in which the platform is used. It constitutes a paradigm shift in the manner in which existing technology is used, new technology is exploited and users interact².

Modern business struggles to operate without being exposed to the internet, even in South-Africa with low internet penetration rate. This trend is driven by the new generation of Internet users entering the workforce (from

¹ On 30 August 2013, Wikipedia (2013) defined Web 2.0 as: "Web applications that facilitate participatory information sharing, interoperability, user-centered design, and collaboration on the World Wide Web. A Web 2.0 site allows users to interact and collaborate with each other in a social media dialogue as creators (prosumers) of user-generated content in a virtual community, in contrast to websites where users (consumers) are limited to the passive viewing of content that was created for them."

² The debate around defining Web 2.0 falls outside of the scope of this research.

university) (Hampton, Goulet, Marlow & Rainie, 2012). These internet users want to find ways to lever of this new technology (Bright & Daugherty, 2012; Lin, Harding & Tsai, 2012). With the growth in Web 2.0, less thought is being given to how access is controlled and the impact of access (Faynberg, Lu & Ristock, 2011). The number of internet incidences has increased and consequently more emphasis has been placed on advising the general ‘public’ on the appropriate use of Web 2.0. This increased awareness was mainly driven by popular media. This also had an impact on the modern auditor, requiring them to be more aware of internet risks and related control. In order to react to this, auditing students are taught about the internet risks and related controls. Various new modern teaching tools are used to illustrate the risks and controls to Accounting students. The question arises whether formal education has a greater impact on student’s online behaviour, compared to an awareness gained from popular media.

Section 2 provides an historic overview of evolution of key prior research studies on Web 2.0. This is followed by the problem statement in Section 3. Section 4 documents the approaches used to teach South African Accounting and Strategy students. Section 5 outlines the research methodology employed. The findings are presented in Sections 6 to 7. Concluding remarks are made in Section 8.

2. REVIEW OF HISTORIC RESEARCH LITERATURE

As the popularity of Web 2.0 grew, the popular media published various articles on, for example, security risks relating to Web 2.0, while others focused mainly on business risks (D’Agostino, 2006; Fanning, 2007; Mitchell, 2007). Popular media publications in almost every industry have published some kind of article outlining how Web 2.0 has impacted that specific industry. Most research has been conducted by private organisations such as Gartner, Clearswift, Pew Internet & American Life Project and KPMG, amongst others, with limited academic peer-reviewed research being performed (Shin, 2008). Initially, research focused on understanding the technology, its benefits, uses in a business environment and potential challenges (Clearswift, 2007a; 2007b). Many studies focused on specific applications (such as Youtube, Facebook) and its uses (Chou, Prestin, Lyons & Wen, 2013). Attempts have been made to develop an organisational framework to help businesses to understand and address Web 2.0 (De Hertogh, Viaene & Dedene, 2011). Other research studies focused on the areas of privacy (Cavoukian & Tapscott, 2006), collaboration (Lee & Lan, 2007), and users’ behaviour patterns (Horrigan, 2007; Lenhart & Madden, 2007a & b; Shin, 2008; Smith, 2011).

The most widely used frameworks were developed by Dawson (2008). Rudman (2010a) developed a framework to identify and manage Web 2.0 risks in a company. Before frameworks for risk or value evaluation can be implemented, users’ behaviour needs to be understood. Lardner (1999) argued that the lack of privacy on the Internet could pose an obstacle to the growth of the Internet. Flavian and Guinaliu (2006) analysed the effect of privacy and perceived security on the level of trust shown by consumers on the Internet. They found that an individual’s loyalty to a website is linked to the level of trust. The trust associate with the Internet is particularly influenced by the security perceived by consumers regarding the handling of their private information. Consequently, the level of trust can be evaluated from the types of information posted on Web 2.0 sites. The more information is posted, the higher the level of trust and *visa versa*.

Much work has been conducted on users’ behaviour, and how users manage their identity and privacy. The Pew Internet & American Life Project conducted a series of studies on various user groups ranging from teens to established employees. Earlier studies (Fox, Rainie, Horrigan, Lenhart, Spooner & Carter) in 2000 focused on the use of the Internet. These international authors concluded that there is a presumption of privacy when users go online and that many users are uneducated about how to manage their identities and the risks they expose themselves too. Many users do not know how to manage their identities, how their identities can be tracked, or how to protect themselves, As a consequence, they unwittingly share personal information about themselves. Early in 2007, when the focus changed to Web 2.0, Lenhart and Madden (2007a) conducted a survey of young people between the ages of 12 and 17 across the United States. The study focused on which sites were used, the reasons for use and how they were used, as well methods to mitigate any potential threats. During April 2007, another study by Lenhart and Madden (2007b) investigated a similar research question. They focused specifically on the information teenagers’ share, on assessing how teens evaluated the vulnerabilities, and the relationships online. Researchers found that most teens protect themselves by limiting the information they share and to whom, yet rely very little on automated protection.

Guess (2007) investigated how college students use Information Technology (IT) and its impact on improving the learning experience. He noted a change in the reasons why students were using the Internet, as well as the tools being used. He found, for example, engineering and business students relied more on spreadsheets and graphics editing tools on the Internet. This confirmed comments by Horrigan (2007).

Later research focused on business users' behaviour in general (Clearswift, 2007a), as well as industry-specific business users such as human resources professionals (Clearswift, 2008), health care industry (Chou, Prestin, Lyons & Wen, 2013). Clearswift (2007a) investigated the impact of Web 2.0 on security, and while conducting the study also investigated usage patterns and management of identity of employees in the United States and the United Kingdom. Researchers focused on the type of service most frequently used, the time spent, as well as most prominent risks and related safeguards to mitigate any risks. Another study conducted by Clearswift in 2008, investigated the attitude of human resources professionals to Web 2.0 and how they had adapted Web 2.0 to their organisations. Authors found that organisations perceived risks in allowing employees uncontrolled access to Web 2.0, and although many sites have security features, many users were unaware of the features or did not enable these features. Rudman (2010b) wrote a paper on the incremental risks in Web 2.0.

These studies highlight the importance of identity management and risks in an international mature context. These research studies treated each group as a homogenous group. In this research there is an implied assumption that the users are informed and aware of the risks and safeguards relating to Web 2.0. However a similar study taking user knowledge explicitly into account has not been conducted.

3. PROBLEM STATEMENT

The introduction of Web 2.0 and the increasing number of online threats have resulted in emphasis being placed on Web 2.0 risks and its related controls, which inherently changed user behaviour. The general public and specialist industries have reacted to this change. The number of articles in the popular media on the risks and controls of Web 2.0 have increased. Similarly, the auditing profession has reacted by specifically including online risks and related controls into the Accounting curriculum. The question arises as to whether formal teaching of risks and controls relating to Web 2.0 has a greater impact on user behaviour than simply having an awareness obtained from popular media. The primary objective of this research is to identify whether differences exist in the Web 2.0 usage behaviour of educated compared to uneducated users. The secondary objective is to establish whether being educated on the risks and controls of Web 2.0 influences users behaviour in terms of: (i) awareness of; and (ii) the manner of interacting with Web 2.0.

The study investigates students, because they are the future business IT users, and are arguably the most connected Internet users in South Africa because they are accustomed to having access to computer facilities on campus and are the early adopters of technology. In many instances they are responsible for introducing new technologies to businesses (Clearswift, 2008). Students majoring specifically in Accounting, as well as Business Strategy (as a proxy for educated and uneducated users, respectively) are considered. Accounting students are taught about the risks and controls of Web 2.0 as part of their Auditing module, whereas Business Strategy (refer to as Strategy hence forth) students are not. The Accounting students are taught using various methods and technologies, whereas Business Strategy students are exposed to Web 2.0 only via popular media or their own research. It is important to understand which delivery mechanisms have the greatest impact on how Web 2.0 users manage their identity. The results will help business determine whether formal education or learning-by-doing will aid in the adoption and diffusion of Web 2.0.

4. METHODS USED TO TEACH WEB 2.0 RISKS AND CONTROLS

The Strategy curriculum does not include IT as a subject, while Accounting students are taught the risks relating to the Internet, as well as related safeguards, in both their IT; Auditing and Governance courses. Strategy students will only be exposed to IT risks and methods to mitigate the risk from popular media or by their own research. The Accounting students are not only taught about the risks and controls, they are also taught a framework to identify risks and formulate controls. Teaching is mainly face-to-face, with all under- and post graduate modules being blended, using compulsory online activities, business cases and additional reading. The following study aids were used in Accounting lectures to illustrate the risks and mitigating controls:

- Textbooks and detailed class examples of risks and controls, as well as examples of what can go wrong if systems and controls are not implemented;
- Screenshots showing pictures of the controls;
- Illustrations of walkthrough tests and class discussions on the do’s and do not’s;
- Class examples and homework assignment questions; and
- The students were assessed using a theoretical company highlighting the importance of governance; and of using frameworks to learn.

The students were not only taught by means of examples, they were also taught using a principled based approach which would allow them to understand any technology, identify weaknesses and recommend controls to mitigate the consequences.

5. RESEARCH METHODOLOGY

A literature review was undertaken to identify existing research on online users’ behaviour; Web 2.0; risks and controls. This literature formed the basis of a questionnaire. A web-based survey was conducted among students majoring in Accounting, as well as Strategy (as a proxy for educated and uneducated users) in the Faculty of Economic and Management Sciences at a South African university to assess the practices they employed when using Web 2.0. The questionnaire investigated how the students’ manage their Web 2.0 identity and their usage patterns; and evaluated the users’ awareness of the risks relating to Web 2.0 and how they manage these risks. Particular consideration was given to the risks and safeguards the students are taught in class. Before the questionnaire was distributed to the target student population, the questionnaire was reviewed by lecturers in the field of Strategic management; Information systems, Auditing; a statistician; and ten volunteers from the target population. They considered the logic and ambiguity of the questionnaire. Minor amendments were made based on their feedback. The responses were scrutinised to eliminate incomplete responses, while cluster analysis was performed on the open-ended questions.

6. TARGET POPULATION

The target population allowed the researchers to identify whether Accounting students employ better online practices as they become more technology literate and aware of the dangers of Web 2.0 through their studies, as opposed to Strategy students, who are arguably less computer aware users. The nature of the two courses has an impact on how students learn and what students use to learn. Accounting students have a structured course (set by an external accreditation body) with limited need for students to access online resources for class. These students are not required to perform additional research on the course material. Most of the learning material is prescribed and provided to the students. The Strategy students, on the other hand are taught in a less structured manner and the course content is determined by the lecturer. They place greater reliance on case studies, simulations, projects and self-study and their own research. The Strategy course carries a lower credit weighting, which requires them to spend less time working. Accounting course is known for being a more rigorous course, not only taking up more time, but is also more onerous, requiring students to memorize the work and understand principles. Table 1 highlights the key differences between the two groups of students.

Table 1: Key Characteristic Traits of the Two Groups of Students

Accounting	Strategy
Risk averse	Risk aware
Followers	Leaders and strategists
Likes structure	Abstract and work in an unstructured environment
Employees	Entrepreneurs
Independent workers	Collaborators
Not required to do research	Able to perform independent research

In total, 3 219 invitations to participate in the study were sent to students. Altogether 751 students completed the questionnaire. The response rate of 23.3% is considered sufficient to arrive at the necessary conclusions, in light of the exploratory nature of this research. Table 2 reflects their response rates.

Table 2: Population and Response Rates of Two Groups of Students

	Population	Responses	Rate	Overall Rate
Accounting	2944	660	22.4%	23.3%
Strategy	275	91	33.1%	

7. FINDINGS

The respondents were questioned about the nature of Internet use before specific consideration was given to Web 2.0 related matters.

7.1 Respondents’ Profile and Internet Activity

The 660 Accounting respondents comprised 54% male and 46% female students, of whom 71% were white, 24% black (5% preferred not to indicate ethnicity). The major (58%) of the Strategy respondents were females, 65% of the respondents were white (13% preferred not to indicate ethnicity). The demographic profile is not as important as the respondents’ connectivity, because all respondents, other than using their cellphones, have access to the same resources at University (high-speed access points) (Table 3).

Table 3: Main Source of Internet Access

	Accounting	Strategy	Average
University Facilities	66.6%	69.0%	67.8%
Place of Residence	29.7%	31.0%	30.4%
Other	4.0%	00.0%	4.0%

The source of access had a direct impact on the frequency at which the respondents accessed the Internet and the time spent online. Although Strategy students spend more time online, Table 4 (Panel 1 [P1] and 2 [P2]) shows that both groups actively make use of Web 2.0 and that it is a favoured activity. 76% of the Accounting students indicated that they accessed Web 2.0 sites at least once a week. This is compared to 95.3% of Strategy students. 50% of the Strategy students spent in excess of 3-4 hours per week on these sites, whereas Accounting students have a longer tail distribution of average time spent on the internet. 21% of the Accounting students did not know how much time they spend online in the average week. It could be argued that when student indicated that they ‘do not know’, it means that they in actual fact spend a lot of time online, which might change the distribution. Detail as to the proportion of social compared to academic use was not established.

Table 4: Usage Patterns

P1: Frequency of Usage	P2: Regularity of use in an Average Week		Accounting	Strategy
	Accounting	Strategy		
Several times a day	15%	63%	15%	25%
Once a day	24%	17%	11%	13%
A few times a week	28%	11%	9%	21%
Once a week	7%	5%	12%	19%
Once a month	4%	0%	17%	16%
Less than once a month	2%	2%	11%	4%
Do not access these sites	2%	0%	4%	0%
Ad hoc access as required	3%	0%	21%	2%
Don’t know	15%	2%		

The difference in number of accesses per period is attributed to the fact that the Accounting course is the more onerous and time consuming course of the two. The strategy students have more time available and hence spend more time online. Howe (2008) and Carr (2008) argued that availability, access and use of Web 2.0 have changed behaviours and that it has the potential to spur significant changes in how users conduct themselves socially, at work and while studying. This could have implications for organisations, as the students, once employed, would have direct access online from their workplace at which time the usage pattern and behaviour has already been established.

7.2 Nature of Most Frequently Visited Sites

A summary of the most frequently visited sites is presented in Table 5. It is interesting to note that the sites with a direct communication component are used more often than content driven services by Accounting students, while Strategy students reflect a different usage pattern. They present a more even distribution of use across all types of sites. Social networking sites rank second to e-mail usage for both groups of students. These patterns can be explained by:

- The difference between the usage of the two types of personal communication platforms could be attributed to the fact that open communication platform usage is under estimated, because mobile access is not considered as part of the study. Many South-African students access social media from their cellphones. It is interesting to note that the sites with a direct communication component are, irrespective of course, used more often than content driven services. This might be attributed to the high communication costs in South Africa.
- The nature of the two courses impacts on how students learn and which resources they use to learn. As noted, Accounting students have a structured course with limited need to access online resources for class, whereas Strategy students are taught by means of case studies *etc.* and requires them to do research.
- The Strategy course carries a lower credit loading, which require students to spend less time working, giving them more time on the internet, possibly for entertainment purposes. Accounting students do not have time.

Table 5: Most Frequently Visited Types of Sites

Type of Sites	Accounting	Strategy
Personal Communication		
<i>Closed One-On-One Communication such as Webmail and Instant Messaging</i>	40.7%	19.9%
Webmail (e.g. Gmail, Webmail)	32.8%	12.0%
Web-based Instant Messaging (e.g. MSN Web Messenger)	7.9%	7.8%
<i>Open Communication such as Social Networking Sites</i>	27.8%	12.8%
Social networking sites (e.g. LinkedIn, Facebook)	27.8%	12.8%
Information Source		
<i>Passive Interaction Information Sources</i>		
Online encyclopaedia and information sources (e.g. Wikipedia)	15.7%	19.3%
Blogs	13.3%	12.4%
	2.4%	6.9%
<i>Active Interaction Information Sources</i>		
Forums	4.4%	18.9%
Really Simple Syndication (RSS) feeds (e.g. Newsvine)	1.8%	6.1%
Podcasts	1.4%	7.1%
	1.2%	5.7%
<i>Sharing Sites</i>		
Online video sites (e.g. YouTube)	4.8%	11.2%
Photo sharing sites (e.g. Flickr)	4.1%	6.5%
<i>Online Applications, Services and Worlds</i>		
Online applications (e.g. Thinkfree, Smartsheet)	2.0%	5.9%
Virtual worlds (e.g. Second Life)	0.6%	5.3%

7.3 Awareness and Utilisation of Web 2.0 Services

Although a wide range of services are used, 82% of the Accounting students were not always aware that they were using Web 2.0 services. The Strategy students had a greater awareness (49.2%) of Web 2.0 services they use. Both groups of students were able to identify Web 2.0 and could correctly list the differentiating characteristics of these sites. This is important because the changes in technology, give rise to new risks and new safeguards. Figure 1 and 2 reflects the activities performed online and concurs work by Guess (2007) and Horrigan (2007).

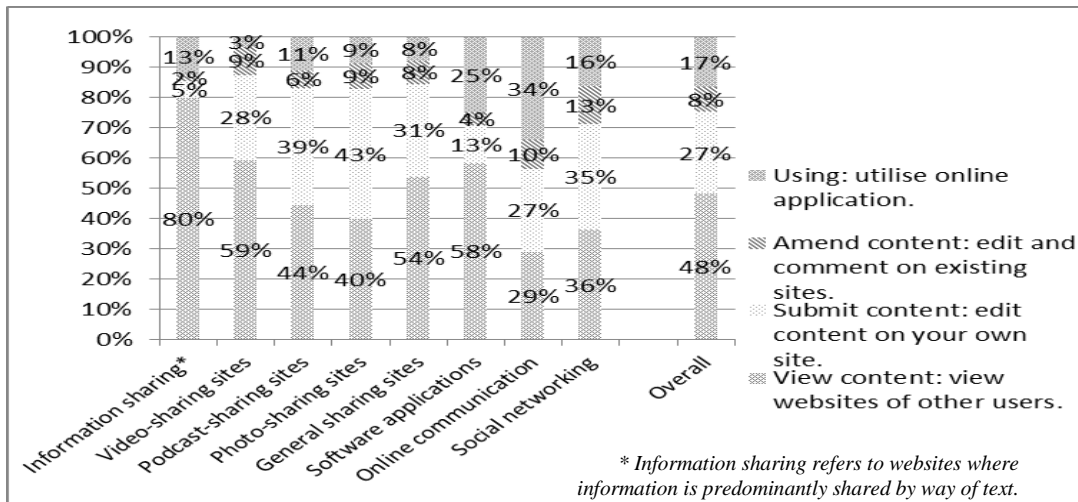


Figure 1: Methods of Interacting with Web 2.0 by Strategy Students

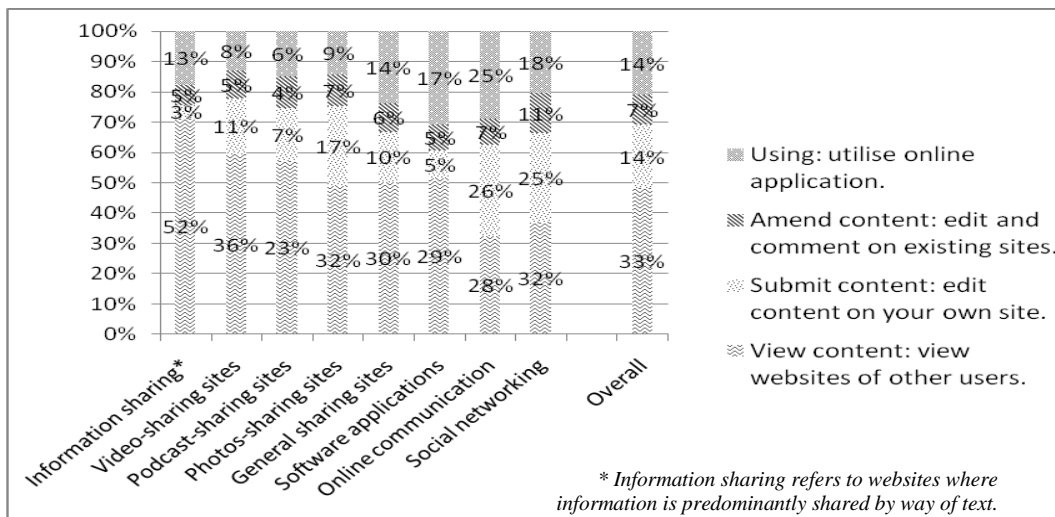


Figure 2: Methods of Interacting with Web 2.0 by Accounting Students

More than half of the students (53.3% - Accounting; 77% - Strategy) indicated that their main activity on the internet is to view content. A significantly smaller portion of Accounting students indicated that they submitted (15.0%) and amended (8.4%) information online, while 23.3% make use of online applications. The Strategy students showed a similar profile with 16.4% submitting information; a slightly higher percentage (18.0%) amending information and comment on Web 2.0 sites; while 24.6% used online applications.

7.4 The Influence of Web 2.0

Web 2.0 uses more resources such as bandwidth and time because Web 2.0 is typically more media rich than Web 1.0 and could therefore negatively impact students and others. Table 6 investigates the effect of Web 2.0 usage on resources.

Table 6: Impact of Time Spent on Web 2.0 Sites

	Accounting	Strategy
Does not influence the university's resources.	30.5%	33%
Does not influence other students and colleagues.	57.4%	58%
Influences on a students' studies.	46.0%	47%
Does not influence a students' social life.	48.2%	43%

Both groups responded similarly and were of the opinion that Web 2.0 usage did not influence university resources, but did impact on other users. This might be because the majority of the students used the university’s facilities to go online. Under half of the students believed Web 2.0 usage influences students’ studies by taking up study time. The result, taken in conjunction with the nature of the Web 2.0 services used, may indicate that the effect will be predominantly negative. It appears (from Table 5) that Web 2.0 is for most part used for social networking, communicating and entertainment, none of which are primarily academic in nature. Web 2.0, therefore, potentially takes time away from academic endeavours. The respondents were divided on the effect on their social life, believing that Web 2.0 influences their social life and the ways in which they interact socially.

7.5 Risks and Consequences

Unproductive time and resources constitute only one risk. Both groups of students stated they were aware of the risks pertaining to Web 2.0 access and the possibility that access may open themselves up to threats. New threats have been developed specifically to target Web 2.0, but Web 2.0 did not change online risks as a whole, it changed the manner in which the threats are delivered. A detailed list of all risks and safeguards is contained in Rudman (2010b). It appeared that Strategy students (75.8%) were more aware of the risks in Web 2.0 compared to 65.3% of Accounting students that stated that they were not aware of the risks posed specifically by Web 2.0. This is contrary to expectations and can be surmised that this is due to the fact that the Strategy students are not able to distinguish between Web 1.0 and Web 2.0 sites and therefore overstated their knowledge and are not aware that the risks are different. Accounting students are taught about the vulnerabilities that affect Web 2.0, being distinct from Web 1.0 vulnerabilities. They might understate their knowledge.

The two groups of students were required to rate seven potential risks, where ‘1’ was the most significant risk and ‘7’ was the least significant risk. Table 7 contains the average ratings for the risks. Irrespective of whether the students were taught about the risks or not, neither of the ratings reflected theory and what students are taught in class. The Strategy students rated the risks higher. The most significant risk, according to the Strategy students, was the possible breach of security controls, while the Accounting students indicated electronic intrusion (including embedded intrusion) as a major risk factor. The last three risks were rated relatively low by both groups of students.

Table 7: Average Ranking of Risks by Two Groups of Respondents

	Accounting	Strategy	Theory
Electronic intrusion	1.96	2.8	Easiest controlled
Phishing attacks, including spam	2.63	2.8	Easiest controlled
Breach of security of website controls	2.64	2.5	Greatest business and audit impact
Information leakage and brand damage	2.92	2.6	Small or no audit impact
Unproductive time	3.38	4.2	Small or no audit impact
Content errors on websites	3.40	4.0	Small or no business impact
Denial of service	3.59	4.0	Greatest business impact

Irrespective of whether the students were taught about the risks or not, neither of the ratings from both groups of students reflected the theory according to the textbook and what the students are taught in class. The students rated the risks that according to the textbooks are the easiest to control, the highest and the risk that has the greatest business impact, as the least risky.

7.6 Inappropriate Disclosure of Information

Many of the risks presented in the previous section arise from sharing too much information. Approximately 80% Accounting students and 98% Strategy students believed they share too much information. In sharing information online, two types of personal information could be posted: (1) when creating a profile or (2) through posting on websites. Both groups of students post similar information online when creating a profile. It does however appear that the Accounting students are more averse to posting information as highlighted by the lower percentages in Table 8.

The students indicated that when they created profiles, they are most likely to share personal information, followed by information about where they reside, followed by contact information. They were less likely to share

content that is resource intensive (to upload or stream files), possibly due to cost implications rather than security concerns.

Table 8: Nature of Information Shared when Creating a Profile

	Accounting	Strategy		Accounting	Strategy
First name	94.50%	98.4%	Student e-mail	39.20%	40.8%
Last name	87.50%	90.6%	Personal e-mail	36.60%	38.1%
Photos of yourself	83.00%	92.2%	Contact numbers	21.40%	28.1%
Name of university	77.20%	87.5%	IM screen name	20.70%	15.6%
Photos of friends	70.80%	79.7%	Current address	19.30%	15.6%
Place of residence	70.20%	73.0%	Videos	13.80%	17.2%
Full date of birth	68.20%	65.6%	Employer details	6.60%	17.2%
Hobbies	57.50%	57.8%	Streamed audio	6.00%	4.7%
Name of school	55.40%	73.4%	Links to blog	3.70%	0.0%
Likes and dislikes	52.60%	68.8%	Work e-mail	3.50%	20.3%

In light of the responses above, the students were asked which types of information they disclosed either on their own or someone else’s Web 2.0 sites (Table 9). It should be noted that this refers to information which they would disclose on their own or somebody else’s website, and not information that is used to create online profiles.

Table 9: Nature of Information Shared on Web 2.0, Other Than When Creating Profile

	Accounting			Strategy		
	Yes	No	Maybe	Yes	No	Maybe
Biographical Information						
Gender	85%	9%	6%	93%	3%	3%
Age	75%	13%	11%	72%	16%	11%
Town/City	66%	21%	13%	79%	15%	7%
Name and location of university	64%	23%	13%	80%	7%	13%
Parents’ professions	16%	70%	14%	7%	85%	8%
Address, home telephone number, parents’ names	13%	72%	15%	19%	73%	8%
Contact Information						
E-mail	53%	33%	14%	57%	30%	13%
Area code	30%	58%	12%	31%	64%	5%
Cell phone number	25%	62%	13%	29%	58%	13%
IM screen name	22%	61%	17%	19%	74%	6%
Personal Information						
Areas of interest	62%	23%	15%	64%	26%	10%
Religious affiliation	62%	25%	13%	61%	33%	7%
Personal preferences (movies, food, etc)	62%	24%	14%	75%	16%	8%
Boyfriend or girlfriend status	61%	25%	13%	56%	31%	13%
Pictures or photos	61%	24%	15%	82%	10%	8%
Profession	56%	31%	14%	51%	36%	13%
Pet information	36%	49%	15%	16%	77%	7%
Physical appearance	34%	44%	22%	23%	68%	10%
Sharing your experiences about your life	33%	48%	19%	41%	43%	16%
Gossip	25%	57%	17%	11%	75%	13%
Personal identification information	10%	82%	8%	3%	89%	8%
Passwords or combinations	12%	84%	4%	6%	94%	0%

On a whole it appears that Strategy students are more willing to share information than Accounting students. It is interesting to note that Strategy students are more willing to share biographical information than Accounting students, will being less willing to share personal information online.

Both groups of respondents would be willing to share biographical and personal information and less likely to share all types of contact information. The lower willingness to share information could be attributed to the fact that students do not want to share their personal information because of the fear of being unnecessarily contacted,

rather than because of security concerns. Most would also disclose their e-mail addresses. Over a quarter of the respondents would provide their cellphone numbers and under a fifth would knowingly provide other information that might allow someone to find them easily, such as address, and home phone number.

12% of Accounting students would provide their passwords online and 10% of these students would share personal identification information such as identity numbers, or medical information, even though they are taught about the risks. A significantly lower number of Strategy students would disclose similar information.

7.7 Safeguards to Mitigate Risk

In order to limit the risks, safeguards could be implemented by monitoring, limiting use, self-protection, or policy implementation. Blocking access is a last resort and not always possible. Monitoring and review is advocated as a important high-level control.

Of the students, 39.9% Accounting and 35.9% Strategy students felt that their activities did not expose them to risks requiring them to change their behaviour. Surprisingly, both groups of students reflected similar responses, irrespective of the fact that the Accounting students were taught the risks in class.

60.6% Accounting and 75.0% Strategy students stated that they did take some steps to protect themselves. Table 10 suggests that Strategy students are more likely to implement controls. This confirms findings by Fox et al. (2000) and Lenhart and Madden (2007b).

Table 10: Most Frequently Used Safeguard

	Accounting	Strategy
Use security settings	88.4%	92.0%
Use of policy	82.8%	87.5%
Made information only available to friends	76.3%	89.1%
Password protection	59.4%	79.7%
Providing as little personal information as possible	50.4%	59.4%
Only disclose information to known friends	37.1%	57.8%
Block access	32.3%	33.5%

Slightly under half of the respondents (44.2% - Accounting students; 48.4% - Strategy students) indicated that they would at least limit their activities, if they knew they were being monitored, while 11.6% Accounting students; compared to 7.8% - Strategy students indicated that they would stop using the Internet. Another 4.3% Accounting students and 7.8% - Strategy students felt that with the large volume of online activity, it would be impossible for someone to effectively monitor activities and, consequently, they would not change their behaviour.

Many organisations have Internet policies that govern the use of company resources. The majority of the respondents indicated that they would comply with such a policy, if they were aware of it, while 14.2% - Accounting; 12.6% Strategy students would probably ignore the policy in their use of the Internet. It is noteworthy that the students were required to agree to comply with the university’s Internet policy before they were able to access the Internet using university resources. In spite of this, 3% - Accounting; 1.6% Strategy of the respondents stated that they had never seen such a policy. This would, therefore, indicate that an Internet policy may not be the most effective way of regulating Internet use.

Alternatively, access could be blocked; however, 68% of both the Accounting and Strategy respondents felt that access should not be blocked, even though nearly half (47.2% - Accounting; 36.5% Strategy students) stated that Web 2.0 related risks may impact on the security of the organisation. In addition, 37% both groups of respondents indicated that employees should be entitled to access Web 2.0 content from their work computer for personal reasons, irrespective of the risks.

8. DISCUSSION AND CONCLUSION

Internet security and privacy has received much publicity and with the growing use of Web 2.0, these issues will not abate in the future. Formal user education is seen as the solution, but is not always effective. A survey

was conducted to determine whether differences exist in Web 2.0 user behaviour (including the usage patterns as well as the awareness levels of the risks and controls associated with Web 2.0) of educated compared to uneducated users, by making use of proxies, specifically students majoring in Accounting and Strategy. The Accounting syllabus includes risks and controls of Web 2.0, whereas Strategy does not. The Accounting students are taught using various methods and technologies, whereas Strategy students are exposed to the risks and controls only via popular media or their own research.

The results indicate that the use of Web 2.0 is popular amongst students, they regularly visit Web 2.0, and post personal information irrespective of which course they major in. The Strategy students do however spend more time online and tend to use Web 2.0 sites for many uses, other than communication. The Web 2.0 awareness levels of both populations were relatively high with no significant differences. As far as the potential risks are concerned, both groups of respondents were aware of the risks and indicated that they did take some measures to protect their online identity, but they implemented safeguards in a haphazard manner. Given the distinctive characteristics of the two groups of students, it is expected that differences should be observed between their ranking of potential risks and potential controls.

Contrary to expectation, the level of usage; type of Web 2.0; types of risks; and the manner and frequency of sharing by the two populations were not found to differ significantly. However, Strategy students do tend to rate the risks higher and are more likely to implement controls. This also support an argument that if academics want to make an impact on society, they must write popular articles in their field.

The research highlights that although Accounting students are taught about the risks and controls, they do not consider these risks and controls in their personal life. It appears that being educated on Web 2.0 risks does not have a larger impact on user behaviour than awareness gained from popular media. It might also be argued that popular media could have a greater impact in motivating users to implement controls, because the risks might be viewed as having a real impact. This also says a lot about the manner in which students study and are able to apply theory to practice.

Considerations should be given to blocking access to Web 2.0 and implementing strict controls that do not rely on user implementation, since potential safeguards would, in all probability, be ignored even by informed users or not used. This also says a lot about the manner in which students study and are able to apply theory to practice. When teaching information security, greater emphasis should be placed on practical examples, identification of risks and the real-life implementation of controls relating it to students personal experience. Moreover, organizations cannot rely only on users to employ proper controls.

AUTHOR INFORMATION

Mr. Riaan J. Rudman is a Senior Lecturer in Auditing and Information Systems at Stellenbosch University, South Africa. He obtained his Bachelors of Business Science (Finance Honours) degree as well as a Post-graduate Diploma in Accounting from the University of Cape Town. He also holds two masters' degrees: a Masters of Business Science, in the field of finance and a Masters of Accountancy, awarded *cum laude*, in the specialist field of computer auditing. He is a qualified chartered accountant specialising in Financial Institutions. His areas of interest lie in emerging technologies; business management and acceptable corporate behaviour in an electronic environment. E-mail: RJRudman@sun.ac.za

REFERENCES

1. Bright, L., & Daugherty, T. (2012). Does customization impact advertising effectiveness? An exploratory study of consumer perceptions of advertising in customized online environments. *Journal of Marketing Communications*, 18(1), 19-37.
2. Cavoukian, A., & Tapscott, D. (2006). *Privacy and the Enterprise 2.0*. New Paradigm Learning Corporation. Retrieved from http://newparadigm.com/media/Privacy_and_the_Enterprise_2.0.pdf
3. Chou, W., Prestin, A., Lyons, C., & Wen, K. (2013). Web 2.0 for health promotion: Reviewing the current evidence. *American Journal of Public Health*, 103(1), e9-e18.

4. Clearswift (2007a). *Content security 2.0: The impact of Web 2.0 on corporate security*. Retrieved from http://resources.clearswift.com/Externalcontent/Features/Clearswift/9586/200704SurveyReport_US_1063233.pdf
5. Clearswift (2007b). *Demystifying Web 2.0*. Retrieved from [http://resources.clearswift.com/ExternalContent/C12CUST/Clearswift/9514/200707DemystifyingWeb21\].0_US_1062190.pdf](http://resources.clearswift.com/ExternalContent/C12CUST/Clearswift/9514/200707DemystifyingWeb21].0_US_1062190.pdf)
6. Clearswift (2008). *Content security 2.0: The role of HR and IT in effectively managing the business benefits and risks of Web 2.0*. Retrieved from <http://resources.clearswift.com/main/pages/Clearswift/RSRCCTR/ContentDisplay.aspx?sid=3230&yid=2711>
7. D'Agostino, D. (Winter 2006). Security in the world of Web 2.0. *CIO Insight*, pp. 12-15.
8. Dawson, R. (2008). An enterprise 2.0 Governance Framework-looking for input! Retrieved from http://rossdawsonblog.com/weblog/archives/2008/2/an_enterprise_2.html
9. De Hertogh, S., Viaene, S., & Dedene, G. (2011). Governing Web 2.0. *Communications of the ACM*, 54(3), 124-130.
10. Fanning, E. (2007). Security for Web 2.0. *Computerworld*, 3 September, 44.
11. Faynberg, I., Lu, H., & Ristock, H. (2011). On dynamic access control in Web 2.0 and beyond: Trends and technologies. *Bell Labs Technical Journal*, 16(2), 199-218.
12. Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., & Carter, C. (2000). *Trust and privacy online: Why Americans want to rewrite the rules*. Pew Internet & American Life Project: Washington, D. C. Retrieved from <http://pewinternet.org/Reports/2000/Trust-and-Privacy-Online.aspx>
13. Guess, A. (2007) Students' 'evolving' use of technology. *INSIDE HIGHER ED*. Retrieved from <http://www.insidehighered.com/news/2007/09/17/it>
14. Hampton, K., Goulet, L.S., Marlow, C., & Rainie, L. (2012). *Why most Facebook users get more than they give*. Pew Internet & American Life Project: Washington, D.C. Retrieved from <http://www.pewinternet.org/Reports/2012/Facebook-users.aspx>
15. Horrigan, J. (2007). *A typology of information and communication users*. Pew Internet & American life Project. Retrieved from http://www.pewInternet.org/pdfs/PIP_ICT_Typology.pdf
16. Lee, M., & Lan, Y. (2007). From Web 2.0 to conversational knowledge management: Towards collaborative intelligence. *Journal of Entrepreneurship Research*, 2(2), 47-62.
17. Lenhart, A., & Madden, M. (2007a). *Social networking websites and teens: An overview*. Pew Internet & American life Project. Retrieved from http://www.pewinternet.org/~media/Files/Reports/2007/PIP_SNS_Data_Memo_Jan_2007.pdf
18. Lenhart, A., & Madden, M. (2007b). *Teens, privacy, and online social networks*. Pew Internet & American life Project. Retrieved from <http://www.pewInternet.org/pdfs/PIPTeensPrivacySNSReport.pdf>
19. Lin, H., Harding, J., & Tsai, W. (2012). A rule-based knowledge system on semantic web for collaboration moderator services. *International Journal of Production Research*, 50(3), 805-816.
20. Mitchell, R. (2007). Web 2.0 users open a box of security risks. *Computerworld*, 26 March, 32.
21. Reports/2011/WhyAmericansUseSocialMedia.pdf
22. Rudman, R. (2010a). Framework to identify and manage risks in Web 2.0 applications. *African Journal of Business Management*, 4(13), 3251-3264.
23. Rudman, R. (2010b). Incremental risks in Web 2.0 applications. *The Electronic Library*, 28(2), 210-230.
24. Shin, D. (2008). Understanding purchasing behaviour in a virtual economy: Consumer behaviour involving currency in Web 2.0 communities. *Interacting with computers*, 20, 433-446.
25. Smith, A. (2011). *Why Americans use social media*. Pew Internet & American life Project. Retrieved from <http://pewinternet.org/~media/Files/>
26. Trevathan, J., & Myers, T. (2012). Anti-Social Networking? *World Academy of Science, Engineering & Technology*, 72, 127-135.
27. Wikipedia. (2013). Web 2.0. *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Web_2