Acceptable Use Policies as a Defense Against Threats Posed by the Use of Social Networking Sites in Organizations

Frank H. Katz
Armstrong Atlantic State University
Department of Information Technology
11935 Abercorn Street
Savannah, GA 31405
912-344-3192
Frank.Katz@armstrong.edu

ABSTRACT
From its humble beginnings as a directory of incoming students named thefacebook.com at Harvard in February 2004, to a mega-site used by the campaign of Barack Obama to harness the power of the youth vote, Facebook has become an international phenomenon. Along with myspace.com, Linkedin.com, and others, social networking web sites have changed the way people relate and keep in touch with each other. Indeed, I have joined facebook and use it to keep in touch with friends and relatives, including my son who is away in college. Originally restricted to persons with an .edu e-mail domain, by September 2007, facebook was opened up to anyone who wanted to join. However, the advent of any method of electronic communication brings with it vulnerabilities and threats that may offset some of its advantages. The use of social networking sites such as facebook in businesses, universities, and organizations bring its own particular set of threats.

This paper describes the results of my investigation into the various threats posed by the use of social networking sites in the workplace, and the Acceptable Use Policies (AUPs) necessary to mitigate those threats. Using the University System of Georgia (USG) as an example, I will investigate the AUPs at various universities in the USG and make some recommendations where they may be deficient.

Keywords
Information, Information security, Computer security, Internet, social networks, risk assessment, threats.

1. INTRODUCTION - HISTORY
The concept that individual computers linked electronically could provide social interaction and networking has been suggested from the inception of the Internet. Early efforts included Usenet, and Bulletin Board Services (BBS). Usenet was conceived by Duke University graduate students Tom Truscott and Jim Ellis in 1979. Users read and posted articles or posts to newsgroups related to various different topics. BBSs were developed at about the same time, but reached their peak usage in 1996 with the advent of the GUI-based World Wide Web and web-based message boards. Their use has declined steadily ever since. With the advent of the Web, the first web-based social-networking site was Classmates.com in 1995, which is still in use today. Friendster was founded by computer programmer Jonathan Abrams in 2002 and was the first to introduce virtual communities. MySpace followed the next year, along with LinkedIn, which is aimed primarily at making professional connections. Facebook was founded in 2004 and by April 2008 it had overtaken MySpace as the largest social networking site based on monthly unique visitors.

As the use of social networking sites has invaded the workplace, threats such as the divulging of corporate secrets, privacy issues, the possibility of viruses being unleashed upon corporate networks, and the waste of time devoted to maintaining an individual’s “profile” and keeping in touch with contacts have become serious issues. Threats in the use of social networking sites are not limited to the workplace. Universities face issues ranging from copyright violations to “cyber bullying.”

2. SPECIFIC THREATS FROM SOCIAL NETWORKING SITES

2.1 Data Leakage
“Data leakage” doesn’t refer to a technical problem in an organization’s system. Rather it is a term that describes the problem of sensitive organizational data being posted in the public domain without any kind of restriction. In fact, “results of a survey by the National Cyber Security Alliance (NCSA) found that 57% of users of social networking sites such as MySpace divulged critical information about themselves they would not usually reveal. Some experts said that employees could end up putting out secret corporate information in the public domain.” [3]

Employees often divulge their corporate e-mail accounts, corporate phone numbers, and other apparently non-sensitive corporate information. Given that companies allow social networking sites in the workplace in order for their employees to communicate with each other, it is not inconceivable that such information, secret or not, may accidentally appear on such sites. [8]

“Indeed, nearly 60% of all IT managers surveyed by FaceTime Communications reported that their users social-network at the
office. Of those organizations, the ones where more users were using social networking today than six months ago experienced an average of 39 security incidents a month, requiring 24 hours of remediation.” Four in ten of the IT managers in the survey said they had experienced security incidents that were deliberate, while 27% had seen “unintentional release of corporate information” occur. [10]

2.2 Worms, Viruses, and Malware

The arrival of the Koobface virus that hit facebook users in December 2008 has brought home an important warning to facebook users – “the bad guys are coming for you.” [4] Koobface arrives from an e-mail sent by a social networking friend inviting you to view a video. Once the URL is clicked, the virus prompts you to update your Flash player before the video can be displayed. [7] The virus, enanced in a flash_player.exe file transforms victim machines into zombie computers to form botnets. Thousands of students who are not sophisticated enough to see this as a security risk can be coerced to turning their PCs into zombie machines.

Security experts predict that the success of Koobface in using Flash to distribute malware is just the beginning of such attacks. “Using rich-content applications such as Flash files to distribute malicious code has become the latest trend in cybercrime,” says Yuval Ben-Itzhak, CTO of Finjan, Inc., maker of Finjan SecureBrowsing software. [7]

One of the more successful features of facebook can actually expose users to viruses and malware. That feature is all of the ubiquitous applications available on facebook, allowing users to do everything from sending cyber birthday “cards” to various types of “good karma” to friends. When interviewed by Newsweek, Facebook founder Mark Zuckerberg said that “There are a ton of different ways that people can share information, and rather than trying to develop all those ourselves, we wanted to allow anyone worldwide to create any kind of application.” [12]

The advantage is that “thousands of developers, from big companies to kids in dorm rooms, instantly began creating applications that piggybacked on facebook's infrastructure. The new applications could get instant viral distribution, since the News Feed blasts a report to friends every time someone installs a new app (in other words, free promotion). Developers could make money from facebook-embedded apps by taking ads or selling things—without sharing a penny of the proceeds with facebook.” [12]

The disadvantage is that the applications can only be downloaded if a user clicks a button or checks a box that allows its developers to “know who I am and access my information,” which means everything on a profile. [4] While this is a privacy concern, there is also a risk that as scrupulous as facebook and MySpace say they are with regards to security, it is definitely possible that one of these applications, created by anyone, could contain a hidden virus or malware.

2.3 Privacy and Identity Theft, Especially on Campus

Beyond the possibility of downloading malware, there is the definite hazard of compromising one’s privacy. This is a serious problem on college campuses, where the use of social networking sites is pervasive. Either because they are unaware or have not been educated to the threats to privacy, college students are particularly at risk for having private information made public.

Individuals willingly post their birthdates online in sites such as facebook, and then invite members of their family to become their friends. If one of those members happens to be their mother, or better yet, their uncle (mother’s brother), an identity thief would then have that person’s birth date and mother’s maiden name, two “keys to the kingdom” when it comes to identity theft.

Indeed, a “social networker’s friends can, for instance, give access to personal information or photos in a profile. That happened to the call girl involved in the recent sex scandal with former New York Governor Eliot Spitzer.” [4]

“Researchers at Indiana University also published a study last year showing how they ‘scraped’ information from student’s social network profiles, Posing as people’s friends, they then used the information to fool students into providing their university ID and password on a bogus external Web site.” [6]

Phishing attacks attempting to conduct identity theft directed specifically at users of social networking sites is on the increase. According to Symantec’s Internet Security Threat report for the second half of 2007, there were 87,963 “phishing hosts,” which look for personal information about Internet users. The report further states that that figure was not only up 167% from the first half of 2007, but that “66% of phishing attacks in the U.S. were directed towards social-networking sites.” It’s no surprise why social sites are being targeted: “users of these websites are putting up a large amount of confidential information that is being used for fraudulent activity and financial gain,” said Symantec Australia managing director Craig Scroggie. [14]

2.4 Copyright Issues

Social networking sites promote the exchange of information. While most users post photos and information about themselves and their families, there is no doubt that users also post photos and stories that may be copyrighted. In the YouTube era, when any video taken anywhere may be made available on the web, users have to especially careful in what photos, videos, and documents they post online. While the threat of data leakage has been stated earlier, and leaked corporate data might be considered a copyright violation, copyrighted music, photos, and stories available in facebook are not often thought of as “data leakage.”

Often uploaded by college students, the sharing of such copyrighted material using a social networking site could result in the threat of a lawsuit being brought against the entity providing the connection. This has happened to several universities where students, using the university’s Internet connection, have used P2P applications to provide access to copyrighted material. The Recording Industry Association of America (RIAA) has threatened lawsuits if the student accounts used for the P2P activity were not provided to them. The universities had no choice but to comply with the RIAA’s requests.

Since social networking sites provide the capability of downloading or copying files, this scenario could occur if students provide such copyrighted material in those sites. While not a privacy concern, copyright violation is an important issue with any entity providing an exclusive connection to an individual such as a university, business, or organization.

2.5 “Cyberbullying” and Harassment

Long before the advent of the World Wide Web, “bullying” or harassment was limited to face-to-face interaction, whether from a
These universities range in size from Armstrong, which has networking sites among universities, I chose five universities.

The National Crime Prevention Council defines cyberbullying as the use of “the Internet, cell phones, or other devices . . . to send or post text or images intended to hurt or embarrass another person.” Some states have anti-bullying statutes on their books, but mention nothing about the Internet and electronic communications. [11]

“The issue of cyberbullying became the focus of a national debate in 2008, when Lori Drew, 49, was prosecuted in connection with the suicide of 13-year-old Megan Meier in October 2006. Believing Megan had spread rumors about her daughter, Drew and an employee of her small business assumed a false identity of a 16-year-old boy. After winning Megan’s trust, they began sending venomous messages through her MySpace account.” After sending a particularly harassing message, Megan was found later that day hanging from her neck in a closet. She died the next day. Local prosecutors could not find a law addressing Drew’s behavior, and did not press charges. But “a federal grand jury in Los Angeles, where MySpace is headquartered, indicted Drew on charges of accessing protected computers without authorization to obtain information to inflict emotional distress – in other words, violating MySpaces’s terms of use by faking an identity.” [11]

Drew was convicted of three misdemeanor violations of the Computer Fraud and Abuse act, faces up to three years in prison, and will be sentenced in April 2009.

The case has been followed very closely in Internet forums and blogs, and one conclusion from a report in December 2008 by a task force appointed by the 50 state attorneys general and directed by the Berkman Center for Internet and Society at Harvard was that while “online sexual predation of minors generated more headlines, ‘bullying and harassment, most often by peers were the frequent threats that minors face.’” [11]

One solution implemented by the school district of Duluth, Minnesota, is to monitor all e-mail sent using students accounts. It also provides parents with monitoring equipment so they can monitor their children’s social networking activities at home. If a student’s e-mail messages include “bullying-type words or inappropriate words in general, then we’ll send that e-mail to an administrator to review it,” said Keith Anderson, the district’s coordinator of media technology. [11]

3. ACCEPTABLE USE POLICIES AT GEORGIA UNIVERSITIES

In my investigation of AUPs regarding security and social networking sites among universities, I chose five universities within the University System of Georgia. They were: Armstrong Atlantic State University, in Savannah, Georgia Southern University, in Statesboro, the University of Georgia, in Athens, Kennesaw State University, in Kennesaw, a suburb northwest of Atlanta, and Georgia State University, in downtown Atlanta. These universities range in size from Armstrong, which has approximately 7,000 students, to the largest, the University of Georgia, with over 33,000 students.

Each university posts policies regarding the use of Information Technology, including information and computer security and use, on their web pages. Each of the universities have statements in their policies regarding the user’s responsibility to ensure the security and integrity of the university’s computer system and network, responsibility to respect others on the network, ensure that viruses and other malware are not released on their networks, and are not allowed to defame and harass other students. However, none of the university AUPs have any specific language regarding the use of social networking sites. Some examples follow.

3.1 Armstrong Atlantic State University

Some of the threats discussed previously are addressed in AASU’s policy. “Users have a responsibility to ensure the security and integrity of the computer and network resources and services they use or access.” It is specifically stated that users are not to use peer-to-peer (P2P) sites such as Kazaa to transmit and share data. The protection of copyrighted materials is addressed by stating that “Copyrighted materials can not be shared by any means without proper permission. This includes sharing via network file shares, the web, or any other means and is not limited to peer-to-peer programs.” [1]

3.2 The University of Georgia

UGA is emphatic that they cannot guarantee the user’s privacy – it is up to the user to ensure his or her own privacy. “Users shall not place confidential information in computers without protecting it appropriately. The University cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by computer unless special arrangements are made.” [15]

In addition, the university is specific about the messages transmitted through their system with regards to fraudulent, defamatory, and harassing messages. “You have exactly the same responsibilities on the computer network as when using other forms of communication. You must obey laws against fraud, defamation, harassment, obscenity, solicitation of illegal acts, threatening or inciting violence, and the like. Bear in mind that uninvited amorous or sexual messages are likely to be construed as harassment.” This is very close to prohibiting activity that could be construed to be cyberbullying. [15]

3.3 Georgia State University

An important element of protection when using social networking sites is the use of passive anti-virus software. Georgia State’s policy requires that “passive anti-virus detection and removal applications will be installed and activated on all Windows or Macintosh desktops, workstations and laptops/notebooks which are either physically or remotely connected to the Georgia State University network.” [3]

Similar to the University of Georgia, Georgia State’s Issue Specific Security Policy (ISSP) regarding ethics clearly states that Users shall not use information systems to engage in harmful activities; such activities include, but are not limited to, Internet Protocol (IP) spoofing, creating and/or propagating viruses, port scanning, disrupting services, damaging files, purporting or representing one's self as someone else” and that “users shall not
use information systems to transmit communications that are fraudulent, defamatory, harassing, obscene, threatening, and that unlawfully discriminate” [9]

3.4 Kennesaw State University
Kennesaw State requires that “All computers which are the property of Kennesaw State University must have the campus-standard antivirus client installed and scheduled to perform a local scan weekly (at minimum). In addition, the anti-virus software and the virus definition files must be kept up-to-date.” [2] However, this is different than requiring that all computers that connect to their network possess anti-virus software. In addition, I could not find any verbiage within KSU’s Information Technology policies that specifically addressed ethical issues as were stated in both the University of Georgia and Georgia State’s policies.

3.5 Georgia Southern University
As does the University of Georgia, Georgia Southern clearly states that users have “no expectation of privacy of materials stored on those resources.” [6] It states that “Computer users should not place confidential information in computers without protecting it appropriately. The University cannot and will not guarantee the privacy or confidentiality of computer files, electronic mail, or other information stored or transmitted by its computers.” [6] Georgia Southern makes it clear that it’s the user’s responsibility to police their messages transmitted across the Georgia Southern network: “authorized computer users shall take full responsibility for messages that they transmit through the University’s computing resources. The University’s computing resources shall not be used to transmit any communications prohibited by law, including but not limited to fraudulent, harassing, obscene, or threatening messages.” [6]

4. RECOMMENDATIONS AND CONCLUSIONS
Given that universities promote free speech, it is would be impossible for a university or college to limit students’ access to social networking sites. Rather, university computer/information technology services departments must not only publish appropriate acceptable use policies, they must educate students about them and then enforce them.

Such policies should specifically state what is and is not appropriate and expected in terms of: requiring the use of anti-virus and firewall software on student computers; privacy; and the content of messages on the network. Students must be made aware that the institution cannot guarantee their privacy and that it is up to them to do so. They must be informed that fraudulent, defamatory, obscene, and harassing messages transmitted on the university’s network will not be tolerated. “Assumptions of anonymity on social networking sites should be challenged.” Users should be reminded that what they post on numerous social networks is accessible to anyone with an Internet connection. [5] Users of social networking sites are often made aware of posts and activities from “friends” via the regular e-mail account that they used to register with the site. Clicking on links in such e-mails may put the user at risk for malware downloads or identity theft. Posting exact birthdates in social networking sites can lead to malware infections. Users should be made aware of these and other dangerous behaviors in university AUPs specifically aimed at the use of social networking sites.

The points described above should be a part of any organization’s AUP regarding social networking sites, whether that organization is a corporate or academic entity.

In order for a policy to be effective, it must be disseminated, read, understood, and agreed to. It is relatively easy to do this in a corporate environment, where employment is often contingent on completing such training, but harder at a university consisting of thousands of students. Universities should consider requiring that students not only take a brief training course in computer/information security upon enrolling, but that they also be required to take refresher training at the start of each academic year. Users should receive certificates or annotations in their permanent record verifying that they completed the course. Universities could make continued use of their networks based on the successful completion of such a course.

While business and academia have different missions, there is no doubt that there is a common need to preserve and protect the security and integrity of information stored in their systems. Social networking sites such as facebook and MySpace can be a benefit in connecting employees and students, but present significant threats to the security of such systems. The best way to protect these systems is to incorporate specific guidelines regarding threats posed by these sites into existing AUPs, and ensure that users at these organizations have read them, understand them, and agree to adhere to them.

5. REFERENCES


[12] Levy, Steven, Facebook Grows Up, Newsweek, August 27, 2007, p.41-46

