Global Information Assurance Certification Paper

Risk Assessment of Social Media

GIAC (GSEC) Gold Certification

Author: Robert Shullich, rshullic@earthlink.net
Advisor: Rodney Caudle

Accepted: December 5th, 2011

Abstract

The use of Social Media introduces many risks to the enterprise. One common attribute of social media and the technology known as WEB 2.0 is *user generated content*. Any web site that enables a visiting user to post content provides an opportunity where an organization can be harmed. Although there are many known social media sites, there are thousands of sites that fall within the definition, serving millions of web pages, and all containing content published by visitors to those sites. Some of the risks that an organization should consider include compliance with regulatory requirements, reputational damage, information leakage, loss of intellectual property, malware attacks, copyright infringement, and privacy breach. The organization should be aware of information posted about it on other sites which can also cause damage to the organization. Proper management of social media usage is required, because even if an enterprise prohibits its use, the employee may find a way to do it anyway - even when using social media at home - and this can still cause headaches for the organization. This paper will describe many of the risks of social media usage so that an enterprise can conduct a risk assessment and determine which risks are applicable to the organization.

1. Introduction

According to a September 2011 survey, 63% respondents indicated "that employee use of social media puts their organization's security at risk" while 29% "say they have the necessary security controls in place to mitigate or reduce the risk" (Ponemon Institute, 2011). In another study 49% of executives surveyed said that they feel that the use of social media could damage company reputation, yet in that study "only one in three companies addressed those concerns" (PRNewswire, 2009). These two studies indicate that social media poses a substantial risk to the organization but the risk itself is not being adequately addressed. For these types of risks the organization has less control because they do not own, manage or controlled the systems involved.

The size and growth rate of some of the more popular social media networks are phenomenal. FaceBook, a social networking site, has reached close to 700 million users (eBIZ MBA, 2011) and looking at the number of users, if FaceBook was a country, it would be the third largest (Hardaker, 2011). According to a brochure released by Websense, FaceBook has an annual growth rate of 41% and Twitter is growing at 85% year after year (Websense, 2011). In 2011 Google released its Google+ social networking offering, first by invitation only and then generally opening the site. Google has not reported the actual number of users but attempts outside of Google to calculate those numbers and predict the Google+ growth rate are showing more than 50 million users within just a few months since launch (Albanesius, 2011). Google's VP of Engineering claimed that in the first month Google+ has 40 million users (Hachman, 2011).

Organizations depend on its workers to use technology to perform their job responsibilities and there is a need to trust these workers to protect company sensitive data. Yet a survey of 2000 respondents indicated that "More than half of all users of social networks in the U.S. are posting information that could put them at risk of being targeted by cybercriminals" (Gaudin, 2010a). How can an organization expect its workers to protect the organization's data when these same employees may not be protecting their own personal data?

In another report McAfee labs predicted for 2011 social media "targeted abuses of personal identity and data" (McAfee, 2010). According to a Sophos December 2010 survey 40% reported receiving malware on social networks, double from an earlier survey in April 2009 (Sophos, 2011a). In an updated min-year 2011 report, a new survey reported 45% receiving malware, and "social networking threats explode" especially with privacy issues (Sophos, 2011b). Websense reported that "52% reported an increase in malware attacks due to employee use of social media" (Websense, 2011). With the widespread adoption of social media, especially social networking, this has become a major attack vector and entry point to infiltrate an organizations network and exfiltrate its data.

KnowBE4 is an organization that provides security training and ran an experiment to run a simulated phishing attack. In that simulation 43% of those receiving the phished e-mails clicked on the link provided in the e-mail (KnowBe4, 2011). On social networking sites users are experiencing 71% of spam and 46% of phishing attacks (Sophos, 2011b) and based on the KnowBE4 test, many users will receive a phished e-mail and will be clicking on those links.

Between 2009 and 2011 a survey shows that more companies are allowing access to social networks, where in 2009 54% prohibited access completely and in 2011 only 31% had a complete prohibition (Meyer, 2011) (Robert Half Technology, 2011). Users are smart, if you block something, they are good at figuring a way to get around it. So even with the social media ban, more employees are visiting those sites at work (Sachoff, 2010). With organizations experimenting with *Bring Your Own Technology (BYOT)* and the Consumeration of IT, implementing technical controls to prevent access to social media websites may prove difficult. It may be smarter to lift the ban and deal with the problem.

A perfect storm is coming together where social media may become a major attack surface for the organization. More companies are allowing the use of social media, and many companies that restrict its use probably have users doing it behind their backs. Spam, Social Engineering and Malware attacks are on the rise, with cybercriminals using social media as a rich source of targets. And the risk is to the business as the bottom line

may be affected due to lost revenue, tainting of the reputation and brand, loss of intellectual property, and increased costs to repair the damage.

Social media provides an attack vector which can enable an attack on the organization. But that is not the only risk. Social media is a tool, and there may be consequences if that tool is not used properly. A firearm is a tool that someone can use to provide protection, but improper use of the firearm could lead to shooting oneself in the foot. Social media can work in the same way. Social media can also be used in a positive way as a tool to make money, enhance the business, or reduce business costs.

The use of social media within an organization needs to be managed, even when such use is prohibited. If social media isn't managed, then outcomes that were intended to be prevented may still occur. Whether the employee brings in a laptop to work and bypasses policy and controls, or conducts the undesirable behavior at home and puts the organization at risk, the organization may be the one to pay in the end. And even in the workplace, without connection to the organization's network or using the company's assets, an employee using a web enabled cell phone or web enabled tablet can still cause havoc while located on the organization's property.

Management of social media requires procedural and technical controls, i.e. policy and technology. One size does not fit all, and that includes the assessment of risk as each organization has a different risk appetite and may take different approaches to risk mitigation, transfer, avoidance and acceptance. The earliest process to be performed should be a risk assessment of social media that will identify the risks showing the threats, possibilities of the threat occurring and the impact on the business should the threat occur.

Part of the risk assessment will be to identify the threats in terms of vulnerabilities and exploits. This is a challenge as the key ingredient of risk is uncertainty. There are common areas of social media risk that should be considered in the risk assessment and should at least provide a good foundation and starting point.

Robert Shullich, rshullic@earthlink.net

2. Scope and Disclaimer

2.1. Scope

The intent of this paper is to address the identification of social media threats. In order to evaluate the risk in using social media, the reader of this paper must be able to determine what things can go wrong. However, this paper can't be a "one size fits all", can't detail every known risk, nor predict what the future will hold.

2.2. Out of Scope

Regulatory compliance and possible legal implications of social media mentioned in this paper are specific to the United States. Legal issues and concerns for international use of social media most likely will be different as other jurisdictions have different customs and laws.

Risk management, including the risk assessment component are very detailed and comprehensive processes. This paper has a narrow focus and will not address the entire risk assessment process.

Since the scope is Pure Risk Analysis, the paper will present a negative view of social media use, sort of a Chicken Little "the sky is falling" position. The benefits and Return on Investment (ROI) of social media use are not addressed.

2.3. Disclaimer

The author is not a lawyer, and information within this paper is not meant to be legal advice. If the reader is faced with a potential legal issue introduced in this paper, the reader should seek the professional services of competent legal counsel.

3. The Definition of Social Media

One definition for the term "social media" is given as "… the set of Web-based broadcast technologies that enable the democratization of content, giving people the ability to emerge from consumers of content to publishers. With the ability to achieve massive scalability in real time, these technologies empower people to connect with each other to create (or *co*-create) value through online conversation and collaboration" (Scott & Jacka, 2011).

A technology related to social media is Web 2.0, a term coined by Tim O'Reilly and made popular after a 2004 conference on Web 2.0 (Bernal, 2010). One common theme of Web 2.0 is ***user generated content***. When integrated with the social media definition above this fits in to the "emerge from consumers of content to publishers". Yet, user generated content existed well before the Internet became public, so it is not a new idea. Users could buy services on various dial-up networks such as Compuserve, Prodigy, and America Online and participate in discussions. These services provided *bulletin boards (BBS)* which were forums for discussions and the sharing of ideas. The users of a BBS were not just presented with content that was displayed and controlled by the forum; those users could make posts and add their own content. This is an example of one class of social media called collaboration. In another view the difference between traditional and social media is the interaction of the user (ISACA, 2010). In the Internet before this Web 2.0 concept appeared, user generated content existed in e-mail, chat, and instant messenger facilities. Forums and discussion groups were ported to the Internet and existed there as well.

Social Media may be segregated into classes of collaboration and sharing, here is one approach classifying social media into 15 categories (Bard, 2010):

- Micro-Blogging
- Publishing
- Photo Sharing
- Aggregators
- Audio
- Video
- Live-casting
- RSS
- Mobile
- Crowd Sourcing
- Virtual Worlds
- Gaming
- Search

- Conversation Apps
- Social Networking

This is just one way to map out the social media landscape. Social networking also provides some overlap. FaceBook provides a chat feature that would fall under conversation apps. AOL instant messenger provides an interface into FaceBook so that a user can participate in a FaceBook chat using the AOL IM interface. And with photo sharing sites in the social media landscape, FaceBook also provides photo sharing where users can post photos and even tag people in the photos. FaceBook as a social networking site integrates many of the other social media categories into one stop shopping.

Another point of overlap is with cloud computing. With the exception of social media hosted within an organization's intranet, all external social media sites are effectively external service providers. In the case of Google Docs collaboration and publishing is moved outside the organization and into the cloud. It is not enough to just manage social networking, the risk assessment and managing of these external service providers should be required as well.

When examining different reports and articles regarding social media risks, there are two common risks that are mentioned often: reputation damage and data leakage (McAfee, 2009) (Symantec, 2011) (Thompson, Hertzberg, & Sullivan, 2011) (Nyman, 2011) (ISACA, 2010) (Goodchild, 2010). Both of these risks are related in one way, as data leakage can cause reputation damage. The context of these findings usually discusses the threat imposed by an employee or other worker within the organization. Reputational damage can also be caused by an outsider. Unlike traditional news media which can be selective about what gets printed, in social media anyone can blog and post information about anyone or any organization. Verification of facts may go unchecked. Social media provides a listening ear for any disgruntled or unsatisfied customer to sound off. An organization might be able to exert some control over their employees, but in the case of a customer making complaints, the resolution requires some form of damage control. Removal of an offending post may be difficult or impossible to achieve, especially if it goes viral.

Figure 1: 15 categories of Social Media according to Bard

4. Risk Assessment

Steve Elky provides a good primer on Information Risk Management in the SANS Reading Room. Steve's paper is heavily based on the *National Institute of Standards and Technology (NIST)* Special Publication 800-30 (Elky, 2006) (Stoneburner, Goguen, & Feringa, 2002). For a definition of risk, NIST states: "***Risk*** is a function of the ***likelihood*** of a given ***threat-source's*** exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization." Steve then states: "Risk is assessed by identifying threats and vulnerabilities, then determining the likelihood and impact for each risk" (Elky, 2006). Another definition of risk: "risk as representing any situation where some events are not known with certainty" (Chavas, 2004). Risk analysis is performed to: "describe these risks (risk assessment), talk about risks (risk communication), and do something about the unacceptable ones (risk management)" (Yoe, 2011).

Each of the four identification components of the assessing risk – threats, vulnerabilities, the likelihood that the threat will occur, and impact should the threat occur – are difficult problems to solve due to uncertainty. Once the risk assessment has

been completed, each risk should be prioritized so that the critical risks are addressed as early as possible. The impact of risks can be addressed using one of four standard techniques: Mitigation, Transfer, Avoidance and Acceptance. These techniques are not mutually exclusive as they can be used in combination with each other. Any risk still remaining after mitigation and transfer is called residual risk and is usually the risk accepted by the organization.

The residual risk that is accepted can also be considered as what the organization is willing to lose, i.e. acceptable losses should the risk event occur. What is considered an "acceptable loss" varies by organization, and this is also called the "risk appetite". Risk is generally classified as "pure" or "speculative" where pure risk only examines losses and speculative risk can lead to profits or losses (Broder, 2006).

The first step in evaluating the social media risks would be to determine the organization's assets requiring protection, and then assess the threats and vulnerabilities that threaten those assets. Threats may be caused by internal (e.g. insiders, employees, consultants) or external (e.g. customers, activists) actors.

5. Risks of Social Media Use

5.1. Reputation/Brand as an Asset

5.1.1. The Impact

An organization's reputation, brand, and goodwill are an asset. If this asset is impacted in a negative manner, then that organization's customers will no longer wish to conduct business with them.

In New York City most food establishments are graded for sanitary conditions in food preparation and storage. (NYC Health, 2011). The outcome results in a letter grade which must be prominently displayed for customers to see. Any grade, other than the highest grade of "A", sits there for all to see like a scarlet letter (Hawthorne, 2004) and becomes a factor in degrading the reputation of the restaurant. Ratings for the quality and taste of food are performed by food critics that report their reviews in the dining section of newspapers or in rating guides (e.g. Zagat (Zagat)).

Many consumers prefer the opinion of others, opinions typically shared by word of mouth. This method of research has been used for a long time, and when the feedback has been good, word of mouth can sometimes be the best advertising.

Now enter social media. Publishing through social media now provides a mechanism for anyone to spread the good news, but also provides a platform for spreading complaints as well. The difference is that with social media the size of the audience is much larger. Complaint sites such as Ripoff Report (Ripoff Report) provide a forum for complaints. Anyone who has a gripe could blog or tweet about it. Or, create a dedicated website like *I Hate Starbucks* (I Hate Starbucks). Even in social networking, FaceBook has fan pages and even those pages can be for haters. There is a FaceBook fan page called: *The I Hate FaceBook Fan Club*. And a large portion of this bad press published on social media is being created on sites and by posters that the organization does not own or control.

An organization should be aware of who is talking behind their back and talking about them, whether the discussion is positive or negative. When bad information gets out there, the organization needs to decide whether the damage can be minimized so that its reputation can be salvaged.

5.2. Information Leakage

5.2.1. The Impact

Information held by an organization is an asset. Information may belong to the organization itself or may be owned by another entity and held by the organization as a custodian of that information. Even the personal information of an organization's customers may require protection.

If this asset is impacted in a negative way, usually referred to as a breach, it may lead to financial losses. Reputation may be depreciated due to loss of customer confidence. If the information falls under regulatory compliance, there may be costs for compliance failure. For example, disclosure of cardholder data for credit cards and regulated by the *Payment Card Industry (PCI) Council* could result in fines, penalties, higher processing fees, and reimbursement for damages caused by the breach. Loss of trade secrets may lead to loss of competitive advantage.

Information about the organization that might be disclosed to unauthorized parties may expose the organization to an attack. This disclosure of information does not need to be malicious. It can be information that is innocently released without the intent of harm but is later used by an attacker for reconnaissance purposes.

The impact of these losses also includes the costs of trying to repair the damage and recover. A large effort is required to restore customer confidence, especially to show that it won't happen again. Since these breaches may happen, there are also costs for proactive behavior in order to prevent the breach from occurring.

In a study two highly rated social media risks were disclosure of propriety information and disclosure of *Personally Identifiable Information (PII)* (Thompson, Hertzberg, & Sullivan, 2011).

5.2.2. Data Loss

Any data held by the corporation may be at risk. This includes propriety information (e.g. internal corporate data, contacts lists, and internal use only data). Serious data loss can include PII or the loss of *intellectual property (IP)*. The loss of PII could result in financial costs for data breach notification and mitigation. A breach of IP, such as trade secrets, can result in loss of competiveness. Unauthorized release of this data through social media should be scored as a high risk.

5.2.3. Piracy and Infringement

IP can include work product in digital form. A book publisher publishes books, and the IP is the contents of those books. If a book is scanned and posted to the Internet as an e-book, the publisher loses book sales because free copies of the book is being sold, traded, or downloaded for free. This type of IP also includes any type of software, digital copies of music (e.g. MP3s), movies, and computer based training videos. The IP is typically loaded into file sharing sites like Megaupload or Rapidshare (These are also called File Lockers). Social media is used to advertise the pirated content and provide the access links to the IP, which is usually posted in blogs, and forums. An organization can issue a "take down" order on infringed IP, which is a legal right provided by the *Digital Millennium Copyright Act of 1998 (DMCA)*, but the first task is to locate the infringing copies. The IP is stored in the cloud, but the links to the IP is provided through social

media, and diligent monitoring of social media is required in order to stay on top of the problem.

Infringement is using copyrighted work that still has a valid copyright and without the permission of the copyright holder. There is an exception in USA copyright law called *fair use*. It is easy to violate the copyright when publishing content to social media unless certain precautions are taken. A very common violation is using copyrighted material both without permission and without attribution of the work to the rightful owner. This is common in social media because content publishers rarely provide references or use any other method of attribution. Music videos and podcasts may violate copyright when other copyrighted music is played in the background (Britt, 2012). This embedded use of copyrighted photographs and images might be considered infringement.

One company (Righthaven) is attempting to locate copyright infringement photos and make a profit by filing copyright lawsuits (Frosch, 2011). If Righthaven is very successful, more of these businesses will surface and there will be more lawsuits. Righthaven had already filed more than 200 lawsuits.

The organization can be put at legal risk if an employee posts or reposts content without permission. If the intellectual property belongs to a client, there could be a claim of breach of contract (PR News, 2010) (Merrill, Latham, Santalesa, & Navetta, April 2011).

5.2.4. Corporate Espionage

"Today's corporate spies are increasingly likely to use malware and social media to steal sensitive data and intellectual property" (Nairn, 2011). A breach of a Trade Secret can lead to an organization's financial disaster. What would happen if the secret formula of Coke got out there? Can those secrets remain safe? There are competitors out there looking to acquire these secrets and the seekers include hackers, competing organizations and state actors (governments). Cyber criminals, intend to steal a company's secrets in order to further their financial gain. Attackers can use social media to directly steal those secrets or use social media as a vehicle to eventually gain access into the organization to acquire them. The impact in the end may be an intolerable loss that can lead up to bankruptcy.

5.2.5. Reconnaissance

The information in the wild about an organization is an exposure, with the impact that planning an attack is made easier for the attacker. Here is an interview scenario:

An interview is held at a federal facility. As with most interviews, towards the end the candidate is allowed to ask questions about the position. In this case, the position is for a network perimeter security engineer. So the candidate asks: "What brand of firewalls do you use?" The response – "we can't tell you until after you're hired". Security by obscurity, not total security, but part of a defense in depth overall philosophy – don't let anyone know what is being used and make it harder to attack it. If the facility used brand X firewalls, and that was to become general knowledge, then an attacker doesn't have to research the attacks of brand Y or brand Z – one step closer to completing an attack.

There are many job search sites (e.g. Monster, Dice) and aggregate job search engines (e.g. Indeed (Indeed) and Simply Hired (SimplyHired)) offer a place to look for a job. Search, as one of the categories of social media by Bard (Bard, 2010), makes reconnaissance easy. If hackers want to plan a targeted attack on an organization, then they could search the job advertisements and look for a technical job for that company. General search sites such as Google and Bing can be used to turn up other useful information. Google Hacking (Long, 2005) is a technique using the search engines to find security holes, and is used by penetration testers. Hackers may have turned the tables on Google and conducted extensive reconnaissance on Google itself, as a prelude to the Operation Aurora attack (Muncaster, 2011).

Social networking creates an exposure point. The professional social networking site Linkedin can provide interesting insights about an organization's technology (Cowley, 2012). A person's profile may directly show experience on specific hardware or software for a current or former employer.

Discussion forums provide a source for determining the technology being used within an organization. Many of these forums are used for seeking help with a technical problem. Sometimes these forums produce faster results than going directly to the manufacturer because forum members help each other out. But if someone posts that they

have a problem with certain technology at the job, then it could be concluded that either that technology is currently in use or in the process of being deployed. And many of these forums allow search engines to index their content, so these forum posts may appear in search engine results.

If someone wanted to perform a physical penetration of a location, such as to break in and cause damage or burglarize the facility, there are tools out there to help. A search engine can be used to get an address. Geotagging in a picture may provide location coordinates. Once the attackers know where their target is located, then a tool like Google Earth can be used to get an aerial view of the facility. If they want to see the front door, Google Street View may be used. After the facility is cased, they can use Google maps or Map Quest for directions on how to get there.

5.2.6. Organizational Financials

The status of the organization's pre-released financials, especially if the organization is publically traded, creates an opportunity for illegal insider trading. This occurs when material non-public information is leaked. An enployee's simple post on a blog or social networking, like "this was a good quarter" or "this was a bad quarter" will most likely affect the stock price. Premature release of the financials in this manner could become a regulatory issue, especially with a Self-Regulating Organization (SRO) or the Securities Exchange Commission (SEC).

5.3. Content Management

5.3.1. The Impact

Information is content, and content management is the vehicle in which information may be disclosed and exist outside the organization. The impact is that negative, inaccurate, embarrassing, or infringing content released to the wild of social media can be harmful to the organization. The exposure issues that need to be addressed include ownership of the content and "content lifecycle management".

5.3.2. Content Taxonomy

One key distinguishing attribute of social media and WEB 2.0 is the concept of *user generated content*. Social media also collects and creates different data about its

users. Schneier defines the taxonomy of social networking data as: Service, Disclosed, Entrusted, Incidental, Behavioral and Derived. The security and privacy requirements for each vary (Schneier, 2010). Content is user generated but is not just the printed word. It can be photographs, images, music and video. Content may have imbedded content (e.g. a video can have imbedded music and display pictures in the same video). For the organization, published content can come back and haunt it. Social media has become an information source for lawyers preparing for litigation and looking for posts that will provide that smoking gun (Berkow, 2011).

5.3.3. Ownership

Ownership of published content is usually owned by the person creating it at the time of creation. Ownership in the United States is established by USA copyright law, and assumes that the ownership of the copyright was not assigned to someone else. The owners of a copyright may waive some of their rights when posting content to a social media site which may depend on the *Terms of Service (TOS)* of the site. The copyright itself might not be lost, but the site where the content is published may reserve the right to republish and reuse the content.

Unpublished content includes the derived content which is information built or collected about the person. It is also the creation of metadata. This information can then be fed into data mining programs in order to build profiles about the person. The results from the analysis would be owned by the social networking site and then sold to advertisers. This may occur without the knowledge or permission of the site's users (Krill, 2011).

When a person takes a photo, the mere act of snapping that picture creates a copyright and establishes ownership of the image. "Sharing it on a social media site does nothing to limit or reduce that fundamental right, according to digital rights expert Mary Luria". Amateurs that post photos to social media are treated differently than professionals that take the photos for a living, and this creates a double standard on how the images are treated (Sullivan, 2011b).\

When information is posted to a blog, is the poster giving up rights and protections that they possessed before posting that information?

5.3.4. Control

Control over published data may be subject to the TOS of the social media site. Unlike ownership, control addresses what the site can do with the data. If the organization does not own the social media site, then what is published there is probably controlled by someone else. The organization may have limited control to request that data be changed or removed. Infringed content, including copyright violations may be removed issuing a "take down" order authorized under the DMCA. The DMCA isn't usually enforceable outside of the USA.

The control of content is lost once it is posted. Posting to a social networking site where the posted content is meant to only go to selected friends may seem protected by the limited distribution to a restricted audience. However, nothing prevents one of those friends from forwarding that post to someone else outside of the original poster's circle of friends (Huffington Post, 2011) (Associated Press, 2011). The same can occur within a group of employees collaborating on a project, it only takes one person to become a leak and forward information to outside the group. And if privacy permissions on a social media site are not set correctly, the data may leak out and become public by default. This can easily happen with FaceBook's "privacy setting du jour" because FaceBook keeps changing the privacy rules and breaking privacy.

5.3.5. Censorship

The owner of a social media site can change or delete content on its site. WordPress might remove someone's blog, especially if there is a valid complaint or a violation of its TOS. WordPress would not be expected to go into a blog and change words in it, but since they control the website there is nothing to prevent them from doing so.

The owner of a blog may allow responses or comments to be posted, but delete specific posts that the owner does not like or agree with. If the blog is posting infringed material, the blog can be taken down by invoking the DMCA (Masnick, 2011). In other countries, where free speech is not recognized, blogs can be censored by the local government as long as the government can exercise some control or influence over the website.

Retaliation is another method of censorship where posted content can lead to the loss of a job, or even the prevention of obtaining the job in the first place. But an organization needs to be careful how it uses social media, especially social networking, to investigate potential and current employees and take action against them. In some cases the organization may be required to adhere to government regulations such as the FCRA or those set by the NLRB.

5.3.6. Moderation – or – The Social Media Police

Content published in print, through newspapers, magazines, books and journals will usually have an editor that provides governance on publishing. Papers published in professional and academic journals may be required to pass a peer review. Publishing of content is subject to legal requirements and ethical standards. Through this review process, the process of moderating the content reduces the risks of violating laws, incurring legal liability such as defamation, and dissemination of inaccurate information. Failure to vet out these issues can lead to lawsuits and tarnish the brand of the publisher. Supermarket tabloids have a less than stellar reputation where their stories don't always follows these standards. A survey about blogging "revealed that bloggers are not taken as seriously as traditional media" (LeMay, 2005).

When publishing in social media, most of the controls of moderation do not exist, there is no "Social Media Police" out there trying to enforce compliance or any rules or laws or even ethics. Anyone can just open a blog on WordPress or BlogSpot and start publishing content, and can do this anonymously since these are free accounts. This creates an environment without consequences (unless they can be traced). Unless the blog post is doing something illegal, having it taken down could be difficult. If it says something negative about the organization, then the statement could be detrimental to its reputation. Style and language is a factor should the posting be favorable but politically incorrect because it may be viewed as offensive. If it is defamatory and the owner can't be located who can be sued for damages? If the post is negative, but inaccurate, can the poster be made to fix it, or retract and correct it?

5.3.7. Permanence

There is no "recall" command for the Internet. Data released into the wild of the Internet may quickly reach a point of no return, and once that point is passed, the sender has lost complete control of that data. Permanence, as defined by Webster is: "the quality or state of being permanent" (Merriam Webster, 2008). Digital data has the property of lasting indefinitely but also without degradation. Unless the data is intentionally changed or suffers damage during its transmission or storage, it will not by itself fade over time.

"By using digital memory…we escape from being forgotten" (Mayer-Schonberger, 2009). Data becomes a legacy because it will live longer than its creator and longer than the person the data is about. And unlike a quart of milk, that data does not have an expiration date. It has no metadata, no tracking mechanisms and no controls. Metadata could provide information of how many times the data was viewed. Tracking mechanisms could indicate where the data has been and maybe who viewed the data. Control mechanisms could provide functionality to prevent copying, limit printing, and provide an expiration date – a self destruct mechanism. But these attributes are not generally used for the short pieces of data used in social media; these are features of *Digital Rights Management (DRM)* that may be more appropriate for a file or at least a larger chunk of content.

As humans, we can forget. But the Internet never forgets. And once that data is released, there is no getting rid of it. Viviane Reding, the Vice President of the European Commission said: "God forgives and forgets, but the Internet never does" (Berwaerts, 2011). Privacy advocates are working to change this problem by introducing a "right to be forgotten". This is being proposed in a new draft of the European Data Protection Directive that "measures will be put in place to allow European citizens' to have their data deleted by private companies" (Whittaker, 2011). Whether this would be enforceable or even technically possible is yet to be seen.

5.3.8. Representation

When an employee speaks – who are they speaking for? Are they speaking for themselves, or for the organization? Whose opinion is being presented? Many organizations should have a "media relations policy" to handle requests from the media.

A liaison or public relations office should receive the request for comment from the media or anyone else outside the organization. The key is that no employee speaks for the organization unless specifically delegated to be an official voice of the company. The purpose for these controls is to make sure that responses are aligned with the organization's goals, vision, management style and best interests.

Now enter social media. An employee of company XYZ posts a blog. Does that blog contain the opinion of the employee, or is it the opinion of company XYZ? How does the reader of the Blog know? This blog entry could be on a company controlled website, or the employee's personal blog site. Is the employee speaking for the company? Is it possible or even feasible to have every social media post be vetted in advance by a public relations office? Running a blog through a pre-approval process might work in theory because the blog might be similar to publishing an article, but this probably would not work in the interactive world of micro-blogging. Rules of blogging etiquette may be required with disclaimers made by the employee so that it becomes known whose opinions are being expressed. With the limited size of a micro-blog (e.g. Twitter with 140 characters) is it even feasible to have enough room for a disclaimer?

5.3.9. Forensics

Forensics may be as difficult to perform in social media as it is in cloud computing. The difficulty is caused by the fact that the service is usually controlled by a third-party. This may be further complicated by additional downstream service providers to that third-party. For example, the file locker service, MegaUpload, outsourced the disk storage to a cloud service provider. The social media site – if not owned by the organization – is run by a service provider, and the organization probably does not have a contract in place or a services agreement with that social media site. The terms of agreement, other than the standard TOS, is almost like a shrink wrapped package of services. It would be very unlikely in today's world for an organization to send over a group of digital forensics first responders to FaceBook expecting to image hard drives from a FaceBook server. This does not mean that forensics can't be performed. The methods and types of information collected could be different and limited.

5.3.10. Archiving

In certain cases of regulatory compliance eligible business records must be archived. The challenge is the extraction and archiving of the content and the state of the content at the time. Prior to the social media revolution this basically involved e-mail, chat and instant messenger. Capturing the content for archiving was easier to accomplish when tools were available. To limit the cost and resources of the archiving effort, the organization might limit its exposure by prohibiting certain access. For example, web based e-mail like free e-mail accounts (e.g. Hotmail, Yahoo and Gmail) might be blocked at the perimeter firewall. Instant messenger (e.g. AOL, Yahoo, and ICQ) may also be blocked. This limits the exposure because if the organization is not allowing it to happen then there should be nothing to address. In risk management terms this is called *risk avoidance*.

Many organizations will take that risk avoidance route by banning social media. Social networking may have e-mail and chat integrated as part of the offering. If use of these features could fall under the business record archiving requirement, then by allowing social media use would require extracting those messages and archiving them. There are vendor solutions available to accomplish this. Application firewalls might be able to block these features so that social networking could be accessed but the message and chat functions are disabled.

Archiving of content can also be used for investigations and can be a source for a forensic examination. It may also be used as evidence of the state of a social media site for litigation. For example, if a blog or sharing website is infringing on a copyright, a snapshot can be taken of the website and any infringed content before the site owner can disable the site or delete the infringing content.

5.3.11. eDiscovery

Extracting and archiving the content from a social media site has its technical difficulties and challenges. Now add eDiscovery requirements that include preservation holds and prevention of spoliation. Discovery of social media content is being recognized by the courts. “A recent case in Virginia is part of what seems to be a growing trend toward the acceptability of social media in civil litigation” (Carlisle, 2011). It is easy to

make sure that the party in control of the social media content saves it and doesn't delete or alter it. If it is not the organization's site, then the organization is not in full control of what happens to the content. What if the owner of the social media site deletes the content? If a lawyer walks into FaceBook with a preservation order, is FaceBook going to honor it? What if everyone leaves the account alone so it isn't altered and then the account is hijacked? Who is then responsible for the changes the hacker makes? Maintaining the preservation hold order may be proportionally limited to the capability and influence of the party that the order applies. The court might not care as there should be a reasonable expectation of compliance, and the definition of "reasonable" might be undecided at the moment.

5.3.12. Stale or Outdated Information

Information released to the Internet can last forever and old information that has outlived its usefulness can create a problem. If an organization released a price list which had a pricing error, there is the risk that a customer might access the incorrect version. This may result in customer dissatisfaction and disputes. This could also occur when a new price list is published because it will be nearly impossible to purge the existence of the old price lists. If there is an error in blog content, the content can be corrected after discovery of the error. The version of the blog with the error may have been copied or mirrored before the correction was made. It could have been archived in the WayBack machine (WayBack) or may show up in cached search results. Google has a cache feature which, when available, allows viewing of a page that was captured at a previous time.

5.4. Privacy

5.4.1. The Impact

Privacy rights may be protected through regulations. Breach of the privacy, which may be due to data leakage, has different impacts. For the organization, the impact of information breaches has been previously listed. For the owner of the information, the person whose privacy has been breached, besides just being bothered, impacts can be as serious as identity theft, or harassment such as cyber bullying and cyber stalking. Beach of privacy of employee's information, especially executives of the organization, may put them at risk of physical harm.

5.4.2. What is Privacy

Privacy is not security and it is not confidentiality. However, security is required in order to protect privacy. Privacy is not absolute confidentiality where information is kept secret from everyone. Privacy is the ability of a person to selectively release personal information about them to whoever they wish. A person wants privacy so they are not disturbed, they want "the right to be let alone" (Warren & Brandeis, 1890), so they might not release their phone number to just anyone; they may request that it be a non-listed number. As added protection, they may also register the number with the do-not-call registry. But they may chose to selectively distribute that phone number to whoever they wish, and that is their choice to do so.

How that information is released in the real world and the virtual world may be perceived differently. A study shows that social networking sites may be changing the perceptions of online privacy (Sullivan, 2011a). FaceBook still has issues with privacy leakage; photos that were marked private could still be viewed (FoxNews, 2011). Some of the "social networking sites are leaking some kind of private information to third-party tracking sites" (Gaudin, 2010b).

Google will favor its own social networking site, Google+ when returning search results. "The change will expose Google+ profiles, as well as posts and photographs uploaded to the network, to hundreds of millions of search users whether or not they have Google+ accounts" (Helft, 2012). If this change is not implemented correctly there could be substantial data leakage. Since Google also has control over Google+, the search engine could gain access to data that normally should not be accessed. This makes setting Google+ privacy settings critical but what if the search engine ignores those privacy settings?

5.4.3. Lack of Awareness

The lack of privacy awareness is when a user publishes content and doesn't understand the repercussions of what they did. The user may not have set any privacy settings, or set them incorrectly – if the social media site even provides such settings in the first place. Not knowing the implications can come back and haunt them (Berkow, 2011) (Krebs, 2008) (CBS News, 2011). One common exposure is completing a profile

for a social networking site and filling in all the information and allowing it to be viewable. Users will allow personally identifiable information about themselves to be published and viewable such as their full date of birth, home address, their place of business, schools attended, mother's maiden name and phone numbers (Gaudin, 2010a). More than half of the users on social networking sites have published personal information that exposes them to cyber attacks (Sachoff, 2010).

Personal information is key pieces of data that can lead to identity theft and can also be used for social engineering attacks. When combined with other information from the social media site such as status messages, an attacker might be able to predetermine the answers to Knowledge Based security questions used in self-service password resets. In order to reduce helpdesk costs, organizations are moving to automated helpdesks where the user can go to a webpage and reset their own password. This can affect the organization if an attacker can determine the answers and break into a system by resetting the user's password. It can also be used by an attacker to gain unauthorized access to the user's bank account which might use Knowledge Based Authentication (KBA). Obtaining this personal information may be part of the reconnaissance phase of a breach; and some of that information was made easily available to the attacker because the user didn't understand the consequences.

5.4.4. Trust (or Misplaced Trust)

Some traditional media such as research papers, journals, and news stories would require the consumer of the material to trust the source. But in the case of privacy it is about trusting the other players. This occurs in social networking because people join together and there is group dynamics. Trust is often assumed but not always verified, and this is partly due to the lack of awareness. The Internet, and social media, also has an anonymous nature, i.e. without verification of the identity of the other party, do you really know who you are talking too?

On FaceBook if someone goes to a celebrity's fan page, how do they know if it is the official fan page or a fake? If they invite someone they know to be a friend on FaceBook, is it really that person? How about if there is a picture associated with the account and they recognize the picture? Could it have been someone who used the picture

to get close to that person? Finally, if it was the correct account, could the account have been hacked and hijacked after the building of the relationship, and now the person in control of the account is really an imposter?

In many cases trust is built and based on assumptions. But creation of the social media accounts can be made by anyone claiming that they are someone else and there is no policing or checking. How can a social networking site such as FaceBook with over 800 million users regulate all of the users and their actions? One of the biggest problems with Internet fraud is the lack of identification. Unlike authentication where two parties are authenticated to each other, in identification the two parties actually know who they are communicating with. In authentication credentials can be stolen or first obtained under anonymous or false pretenses, in identification there is a higher confidence level of who the other person is. Once a trust relationship is established, it is not always static, it may change over time.

The exposure to an organization caused by this unverifiable state of trust is that the trust relationship between the organization and it customers can be exploited and used for scams. The impact may result in reputation damage.

5.4.5. Harassment

Social media can be a medium for personal attacks such as blackmailing, extortion, cyber bullying & cyber stalking. In the case of Megan Meier, she was a teenager who used Myspace and was having a conversation over a period of time with what she thought was a boy who liked her. Changes in the conversation's tone eventually lead to the teen's suicide (ABC News, 2007). In this particular case the other party was someone pretending to be that boy, which also highlights the dangers of the Internet's anonymity and the impact of the creation of fake accounts. It also questions the issue of trust, an issue that manifests when one party assumes the trustworthiness of the other party without any methods of identification or verification.

In 2010, a college student's gay encounter was video streamed onto the Internet and social networking was used as a means to broadcast the video presence and invite others to watch it. The video exposure was attributed to the student committing suicide (Friedman, 2010).

When spies use sex to obtain secret information, they call it a "honey trap". One of the techniques is to establish a sexual relationship with a target, and use that for blackmailing the person to hand over secrets. Honey traps are also used by governments to test their own agents for loyalty (Knightley, 2010).

These same attacks can be easily enhanced to perform extortion, blackmail and provide an easier mark for the social engineer to manipulate. This can lead to many risks to the organization if the target is an employee or someone with access to critical information.

Although the organization may be a target of harassment, the exposure here is that the employees of the organization are the targets. If an employee (or agent) can be compromised, then the employee can be used as an attack vector into the organization.

5.4.6. Location Awareness

In war, potential adversaries will monitor different communications outlets including social media to determine attack targets and to detect imminent attacks. Early concern by the US military in the use of social media on the battlefield included issues of a breach of secrecy, for example a soldier posting the location of their unit or sending a tweet about an upcoming action about to commence. This information could be used by the enemy. It doesn't require an insider to breach this secrecy, as an observer to an action already in progress can jeopardize the operation and the lives of troops. For example, on May 2nd, 2011 Sohaib Athar was sitting in Abbottabad and started a long line of tweets starting with a helicopter hovering over his apartment at 1 am in the morning. He later discovered, but unknown at the time he was doing the tweets, that this incident was the raid on his neighbor Osama Bin Laden (Olson, 2011). This was a secret mission by Seal Team Six – a mission that was almost jeopardized by a tweet.

The feature of being able to locate a person has its advantages: finding missing people, tracing events leading up to a crime, or parents tracking their children via cell phones (Associated Press, 2007) (Reardon, 2006). But tracking people also poses a personal danger to that person. Not just to stalk that person by tracing their moves, but by knowing where a person is at any moment also tells where that person is not. If someone posts on social media that they are at the local supermarket, that also says that they are

not at home, and is almost an invitation for burglars to run over and rob the place. For a while there was a website "PleaseRobMe.COM" that was displaying posts from various social media forums to attempt to educate and provide awareness of the problem. But the problem hasn't gone away. An ABC article cautions about discussing what holiday presents were received and posting of vacation plans because cyber criminals are casing the online neighborhood (ABC Action News, 2011). Not only can cyber criminals become aware of whether someone is away on vacation, but also find out what goodies there are to steal and some users are even posting pictures of those presents. In an organization the policy of not publicizing *out of office messages* due to vacations is sometimes old hat. That type of information is a key piece of information for social engineering attacks. When vacation information is posted on social media, and it can be coupled with where that person is employed, that same information gives social engineers some good information in order to pretext.

On July 20, 2009 in Northlake Illinois Microsoft opened a third generation data center (Miller, 2009). Microsoft runs tours of the facility to a restricted audience that each person is required to execute a *non-disclosure agreement (NDA)*. One of the secrets is the actual location of the facility. The address and location of the facility is not disclosed until the person executes the NDA and is pre-approved as a visitor. This is security by obscurity, but Microsoft, for its own reasons didn't want just anyone to know the location of the data center. Yet the article (Miller, 2009) shows an outside shot of the facility and provides no other information since the data center has no external markings. Now, suppose someone uses a cell phone with a camera to take and post a photo of that same building to a social media site, except the cell phone has a GPS and provides Geotagging. If the social media site doesn't strip metadata from uploaded photos, not only is the picture exposed but the actual location where the picture was taken is uploaded as well. Geotagging provides information that can also be used by thieves and stalkers (Murphy, 2010).

One asset, a personnel asset, of an organization includes the executive staff. This is usually the C-Level positions and may include senior or executive vice-presidents. Protection of this level of personnel may fall under the physical security domain of *Executive Protection*. Knowing where executives are (or have been) and what they are

doing can be confidential. Take a scenario where an executive is visiting a potential target for a Merger and Acquisition (M&A). Inference from this information before it becomes public could be used for insider trading, if the inference leads to material non-public information. Protection of famous and important people could be jeopardized by information disclosure due to a post in social media, especially a Geotagged post of the current location of that person. Although not a social media issue, when President Obama entered the white house there was a concern about him keeping his blackberry cell phone, and one of the three major concerns was "physical location of the device" (Herssner, 2009). This shows that tracking of a government official by any means can cause a problem. Imagine the havoc of disclosure from Geotagging for someone in the witness protection program being posted on a social networking site.

Exposure for the organization is disclosure of the location of assets which are not in the public view but need to be secured.

5.4.7. Social Media as a Investigative Tool

Social media has become another tool for the private investigator (Staff, 2010). Finding out personal information, uncovering fraud and even skip tracing can be mined from social media data. Insurance companies are using social media to investigate insurance fraud especially disability claims (Li, 2011).

Social media has been used for vetting out potential employees and used to keep track of current employees. When Human Resources (HR) or the hiring manager uses social media in pre-hiring decisions, they can run into problems. Social media does not always reflect an accurate profile of the candidate, it may be the wrong person, the information might be inaccurate, posted content may be taken out of context. FTC requirements for use of social media in hiring decisions mandates adherence to the *Fair Credit Reporting Act (FCRA)*, and is no different than pulling a credit report from a credit reporting agency (Fair, 2011). Use of social media even earlier in the search process could lead to illegal discrimination. A study shows that "75% of recruiters investigate candidates online and 70% of these recruiters reject candidates based on their findings" (Mcgahan, 2011). The *Equal Employment Opportunity Commission (EEOC)* "has announced that for actions in employment claims, it will still use the same rules and

regulations for analysis of lawsuits, etc., even if the information the employer is using against a potential candidate or employee was found on a social media website or elsewhere" (Mcgahan, 2011). This statement by the EEOC says that social media as a data source is not an exception, if it is used for an investigation and affects the hiring decision then its use will be considered like any other investigative source during processing a claim.

5.4.8. Applications (e.g. Games)

FaceBook claims to have over 7 million applications. Some applications are games and provide enjoyment to the player and wreak havoc on worker productivity. Two popular games on FaceBook are Mafia Wars and Farmville. But not all applications are game related. These applications are not written by the social networking site and the social networking site doesn't take responsibility for the application's behavior. Testing is usually left to the developer.

Some applications have access to data in the player's profile containing private information that should be protected and kept private. When an application gains access to this data, collects it, and sells it to advertisers the users privacy is breached (Steel & Fowler, 2010). This was privacy that the user assumed (trusted) they had, but instead becomes a false sense of privacy.

Although employee productivity is an operational issue, applications – whether via social media or installed on mobile devices – provide the exposure of information leakage, and may also provide an attack vector for introducing malware.

5.4.9. Regulatory Compliance

Regulations exist in laws such as the Sarbanes Oxley Act of 2002 (SOX), Gramm-Leach-Bliley Act 1999 (GLBA) and The Health Insurance Portability and Accountability Act of 1996 (HIPAA). SOX is about financial integrity while GLBA and HIPAA have a component that addresses privacy. State privacy breach regulations protect PII to prevent identity theft. An industry regulation, PCI, protects cardholder data which is considered PII. The exposure is data leakage, and the results of a breach can be reputation damage, fines, breach containment costs, and possibly civil actions by those whose data was leaked.

Data leakage can occur with records, such as health records. A contractor managed to port 20,000 medical records for Stanford Hospital to a homework help site (Jaslow, 2011). Protected Health Information data leakage is not just releasing personal details by leaking data records. If a celebrity is admitted to a hospital, and a nurse tweets about the admission (and names the celebrity), this is a violation of HIPAA privacy. In a serious bus crash a surgeon treating critically wounded passengers texted a photo of a severed arm to his wife (McFadden, 2011). This was not a breach via social media and might not have been an actual breach unless the owner of the arm was identified in the photo. But there have been examples of doctors and nurses posting this type of material to their FaceBook status pages. In one case, which involved a severed appendage, the patient's chart which clearly showed the patients name was visible in the photo, and that was definitely a HIPAA privacy violation.

The *Financial Industry Regulatory Authority (FINRA)* is: "the largest independent regulator for all securities firms doing business in the United States. FINRA's mission is to protect America's investors by making sure the securities industry operates fairly and honestly" (FINRA, 2012). FINRA issues regulatory notices to provide guidance based on regulations issued by different regulatory entities such as the *Security Exchange Commission (SEC)*, *New York Stock Exchange (NYSE)*, *Securities Exchange Act (SEA)* and the *National Association of Security Dealers (NASD)*. Organizations subject to these regulations have strict recording and monitoring requirements. This is a main source of the archiving requirements for eligible business communications. Social media guidance notices include 10-06 (FINRA, January 2010) and 11-39 (FINRA, August 2011).

The National Labor Relations Board (NLRB) is a government organization that enforces employee rights. According to an August 2011 survey report, the NLRB was investigating "more than 129 cases that involved social media in some way" (Eastman, 2011). The NLRB filed a complaint that "October 2010 calls into question the ability of employers to take adverse action based on online postings" (Gelb, Hall, & Collins, 2011). With this 2010 case, the NLRB is stating that certain content posted on social media may be protected by an employee's right to discuss and complain about working conditions. Positive postings in social media, such as praise for a product or services, may cause issues between the company and the *Federal Trade Commission (FTC)* (Gelb, Hall, &

Collins, 2011). The organization should be aware of what is being said about the organization, who is saying it, and take appropriate action (or no action) depending on the circumstances. To accomplish this task the organization needs to monitor social media.

5.5. Legal

Legal addresses both criminal and civil implications in the use of social media. Since an organization can end up on either side of the litigation fence, either being sued for damages or suing for damages, every concern provided within this paper can lead to some legal issue. Cybercrime can affect the organization, and civil unrest may impact the organization.

5.5.1. Cybercrime & Hactivism

Social media can be a tool for criminal activity. Criminals can collaborate and conspire to commit a crime. Through social media illegal scams can be run, credit card information stolen, intellectual property stolen, people driven to suicide, people stalked, intellectual property pirated, unattended houses and offices robbed.

Social media can be used as a tool for civil unrest and running a riot. In January 2011 the use of social media was instrumental in the civil unrest in Egypt (Boyd, 2011). It reached a point that Egypt had to block the sites, cut off the Internet, and shut down the mobile phone system. In August 2011 with civil unrest in Britain, social media was used "in plotting violence, disorder and criminality" (Goodman, 2011). This type of effect has fueled arguments between *free speech* and the *Internet Kill Switch*. The exposure to the organization is that if these services are shutdown, and the success of the business depends on those services, how can these threats be mitigated?

Social media can be used to commit harassment, including cyber bullying and cyber stalking. Organizations must also provide a non-hostile workplace for compliance of sexual harassment regulations. If a worker is viewing pornographic pictures on their FaceBook albums, this could be considered creating a hostile environment. If the images are child pornography then there are possible criminal charges. Organizations may implement web URL filtering solutions to block sites with this content, but if social media itself is not blocked and these pictures are stored and viewed, the web URL filtering solution may be ineffective to catch this.

There is an impact that different tools may be required that are "social media aware" and integrate with social media usage and access.

5.6. Attack Vectors

5.6.1. Viruses and Malware

Social media sites are served as web pages. That makes them vulnerable to any type of web application attack, including buffer overflows, cross site scripting (XSS), and code injection. For some sites that use a SQL back end, even SQL injection is possible.

Code injection and XSS attacks are easier to accomplish on sites that allow HTML posting but doesn't perform input validation. Posting to social media sites is publishing user generated content, why assume that the content doesn't include malicious code imbedded in that content? And posting nothing but a simple link to a website could be a link to a malicious web site and result in a drive-by download.

With social media there are two attack surfaces to consider. First is the attack upon the organization where social media becomes a vehicle for malware. An organization may be able to protect itself with standard anti-malware tools such as anti-virus and other end-point protection methods. The other attack vector is an attack on social media itself. This attack vector is more difficult to protect when the organization has no control over the commercial social networking sites.

To prove how vulnerable social networking sites such as FaceBook and Twitter were due to unsecured HTTP transmissions, Eric Butler developed a Firefox plug-in called Firesheep which is a sniffing tool that will expose clear text account passwords (Rusli, 2010). In a malware attack, a piece of malware such as Koobface is propagated via message phishing and infects the user's machine (McMillan, 2010), and the machine then becomes a zombie and is added as a node to a botnet (Slattery, 2008). If this occurs on a machine owned by the organization, then that machine can become a zombie and used for click jacking, distributed denial of service attacks, sending out SPAM, and other forms of cyber crime.

The exposure is not really different than typical malware attacks. What is different is that social media is providing a new entry point into the organization.

5.6.2. Scams

Social networking relies on a trust network. In Linkedin in order to be added to someone's network the connection has to be approved. To become a friend in FaceBook requires the friend to be accepted. Some users will accept and connect to anyone, while others are very choosy on whom they allow into their close and tight circle and will carefully vet each and every request. The more restrictive a person is in building their connections, the higher their perceived trust will be for that network.

What happens when one of those close friends gets hacked? This was a close friend, probably very trusted, yet is now an evil imposter. Timm calls this the "evil twin" (Timm & Perez, 2010). The account holder can easily become the target of social engineering by the evil hacker when relying on the original trust relationship. The way this scam works is the hacker uses the compromised friend's account, and contacts the other friends connected to the account. The hacker will pose a con to get the other friends to wire money. Maybe a story that they are out of the country, were robbed, lost their money and identification, and now need cash to be wired. They are a friend, friends want to help friends, in many cases this scam works and the money is wired. Although this scam has shown up on FaceBook, it was also seen with just using standard e-mail (Grover & Goldberg, 2010) (Sutter & Carroll, 2009) (Ragan, 2009).

If someone can be social engineered to send out money in this type of con job, what else can an attacker get? If the hacker has control over an employee's account, can corporate secrets or other data be stolen? If there is trust, how can an attacker exploit that trust? The exposure is how can trust be exploited to gain access to the organization?

5.6.3. Phishing

Phishing is a social engineering attack, it is also used to conduct a scam, and part of its success is the ability to exploit trust. Spear phishing is a targeted attack and is focused towards a specific target. Spear phishing requires reconnaissance of the personnel intended to receive the e-mails. In one approach an organization as a whole could be phished or social engineered using other methods to identify the intended spear phishing e-mail recipients. One example is the identification of the C-Level executives.

In a 2012 threat prediction report by Booz Allen predicted "Increased C-Suite Targeting, senior executives are no longer invisible online" (Booz Allen Hamilton , 2011). Another threat listed in that same report is: "Growing use of social media will contribute to personal cyber threats".

Phishing provides an entry point into the organization. The payload may be an infected attachment or a link to another website. When the e-mail recipient clicks on the provided link they are directed to either a fake web site (e.g. a fake banking site) or to a website that may contain drive-by downloads.

Using social media for phishing attacks flies under the e-mail content filtering radar because these messages don't flow through the organization's e-mail servers. The message can be anything that supports a link, such as a status post on FaceBook or a tweet using Twitter.

5.6.4. Hijacking

Many organizations also use social media to promote their business and may have an official Twitter Account or FaceBook fan page. To get out to current and potential customers the organization may also produce its own blog and distribute podcasts. Social media provides a direct channel to a very large and wide audience. What happens when these accounts and pages are hijacked or defaced? Web site defacement is old news, but when it happens it becomes embarrassing to an organization. Adding insult to injury, imagine a security company having its own web page defaced (Greene, 2000). This prank of 12 years ago against RSA was nothing compared to the major reputational damage that occurred in early 2011 when code related to its SecurID security tokens was compromised (Richmond, 2011). What damage can an organization suffer if any of its official social media outlets get owned and the attacker takes control? These are supposedly trusted channels of communications and what if the attacker starts posting bad things about the organization, or even worse starts putting out fake press releases? The attacker is impersonating the organization, spreading disinformation. How will that affect the reputation? Can it make the stock price go up or down, providing an opportunity for stock manipulation?

Setting up a fake website may be more difficult depending on how the domain registrar vets out applicants. Creation of fake fan pages and fake blogs that would appear to be "official" outlets can be a threat. Many users don't know the difference and may not ask the question: is this real?

When an account on social media is hijacked, this is usually when an attacker breaks into the account and impersonates the owner, such as Timm's "evil twin" concept (Timm & Perez, 2010). In addition to running a con job, there are other actions that an attacker can perform. Probably the most damaging to reputation would be when an attacker adds their own content to the owners account.

5.7. Shortened URL

Shorten *Uniform Resource Locators (URL)* make using social media easier but also introduces a threat (McAfee, 2010). Some services limit the number of characters in a message. Twitter has a limit of 140 characters. When a long URL is to be posted its size may take up most of the message space. If long URLs are embedded in blogs and e-mails the links may get broken (Vilches, 2010). Using a service to shorten the URL solves most of the long URL problems. These services use a short domain name and assign a short unique string to the long URL. A HTTP redirect process linking to the short URL will transfer the user to the intended page. There are many URL shortening services today, three examples are: tinyurl.com, goo.gl and bit.ly.

The exposure created by these shortened URLs is that the URL could be pointing to any web site and cannot be determined by visually looking at the shortened string itself. Although accessing a shortened URL could lead to a legitimate web page, it could also lead to pornography, scams, malicious sites, or other sites that may be undesirable to reach. A malicious site may be sitting there with drive-by downloads just waiting for someone to visit it. Some services provide the ability to preview links in advance, but users may just click on the link and hope that the link works as expected.

Some organizations may just block the entire service since that may be the easiest method depending on the technology deployed. If the deployed URL filtering software is not capable of determining where the redirect will take the user, then these URL shortening services can be used to bypass the URL filtering process.

5.8. Lack of (or inadequate) Policy

Some organizations have no social media controls in place. Statistics provided in the introduction showed 2 in 3 organizations did not have controls in 2009 and 29% in a 2011 report. Policy is not just a paper document that regulates what is and is not allowed. It requires a program with policy documents, technical controls, awareness training, metrics and monitoring. Even in an organization where social media is just prohibited and outright banned, without a monitoring process in place, how does the organization know that there is compliance with the policy?

Not having a formal written policy becomes a threat since it allows the employees to use social media in whatever manner they want, and that might not be the best for the organization. Some of the organization's current policies (if there are any policies at all) may provide guidelines and governance that limit some of the exposures. But do the current organization's policies align with the social media landscape, or do they require some tweaking and tuning? Does the *acceptable use policy (AUP)* need to be expanded for social media? If the policies do require some change, then the results of the risk assessment should provide input on what those changes should be.

5.9. Operational

Excessive employee use of social media in the workplace (ISACA, 2010) can lead to operational risks. When social media sites are accessed with corporate assets or from the corporate network, technical resources are consumed. These resources are in the form of CPU cycles and network bandwidth. For the worker, loss of productivity may be incurred in the workplace even when using personal assets (e.g. worker uses personal cell phone or tablet to access social media).

6. Recommendations

Once an organization has determined its risk exposures, then a decision will be required to select which risks should be addressed. Typical mitigation of security issues fall in the three control areas: Technical, Physical and Procedures. A good starting place is to implement social media *Acceptable Use Policies (AUP)*, either as a separate policy or integrated into existing AUPs. Existing information security policies should be

reviewed and updated as appropriate to fill in any gaps that social media use may have opened.

As part of technical controls the partial blockage of social media sites may require more advanced technology such as application aware proxy servers and next generation firewalls. For example, a filtering solution that is application aware for the social networking site FaceBook can allow access for many FaceBook features but block the usage of applications such as games. Complete blockage to social media sites might be achieved with less advanced URL filtering solutions.

For regulated organizations where message archiving is required, technical solutions should be sought to capture message, e-mail and chat features of social media, especially those integrated into social networking sites. Or, using advanced application aware technology, blocking the use of these specific features so that there will be nothing to archive.

An organization might not be able to control sites where it has no influence. Monitoring of those sites may be in the best interest of the organization so to at least know what is being said about it. Then, at least there can be some damage control. Some organizations contract with a third party to do this research and monitoring. There are even third parties that will search the social media sites for infringed IP and issue the DMCA take down orders.

Training and awareness is essential. Implementation of policies and procedures should be backed with some form of training. Awareness training helps reinforce knowledge of the policies and provides an opportunity to propose best practices. The use of penetration testing may be considered, and may require extensive social engineering to discover the internal threats.

7. Conclusion

For many organizations the use of social media is a “can’t live with it and can’t live without it” situation. A risk assessment should be performed to determine the effects of social media, i.e. what can happen, and if it does happen, how much damage will it cause. The scope of the risk assessment cannot be limited to just the insiders such as

employees. Insiders may be the biggest threat, but they are not the only threat. Evaluation of external agents is also needed because they can produce content that can negatively reflect on the organization. The threats are related and multiple threats may work in concert towards a greater risk. Eventually, in the end, these risks lead to reputational or data leakage risks and these two risks very often appear in surveys of the top five social media concerns. Once the risk assessment is complete, it can be presented to management for the decision on how to address the discovered risks.

8. Author Information

Robert Shullich is a member of the professional staff of SystemExperts Corporation and is a Graduate student in the Forensics Computing program at John Jay College of Criminal Justice (CUNY). He holds a BS and MS in Computer Science from the College of Staten Island (CUNY), MBA from Baruch College (CUNY), and a MS in Telecommunications Networking from NYU/Polytechnic University. He serves on the SANS Advisory Board. With over 40 years in IT including disciplines of Mainframe Operations, Systems Programming, Program Application Development, LAN Administration, Networking, IT Risk Management, Security Architecture and Information Security, he holds many professional computer certifications including: CPP, CISSP, CISSP-ISSMP, CISSP-ISSAP, SSCP, CISA, CISM, CGEIT, CRISC, CEH, CHFI, ECSA, Security+, CASP, CIPP/US, GSEC, GCIH, GCFW, GREM, and GCFA.

9. References

ABC Action News. (2011, December 5). *Cyber criminals search online for potential victims.* Retrieved from ABC Action News: http://www.abcactionnews.com/dpp/news/science_tech/Cyber-criminals-search-online-for-potential-victims-wcpo1323094743496

ABC News. (2007, November 19). *Parents: Cyber Bullying Led to Teen's Suicide.* Retrieved from ABC News: http://abcnews.go.com/GMA/story?id=3882520&page=1

Robert Shullich, rshullic@earthlink.net

Albanesius, C. (2011, September 27). *Google+ Usage Skyrockets, Hits 50 Million Users?* Retrieved from PC Magazine: http://www.pcmag.com/article2/0,2817,2393640,00.asp

Associated Press. (2007, September 28). *Disney Cutting Off Children's Cell-Phone*. Retrieved from FOX News: http://www.foxnews.com/story/0,2933,298491,00.html

Associated Press. (2011, November 8). *Judge Rules Teacher Should Lose Job After Facebook Post*. Retrieved from Fox News: http://www.foxnews.com/us/2011/11/08/judge-rules-teacher-should-lose-job-after-facebook-post/

Bard, M. (2010, February 8). *15 Categories of Social Media*. Retrieved from Mirna Bard: http://www.mirnabard.com/2010/02/15-categories-of-social-media/

Berkow, J. (2011, December 7). *Beware social media :What you tweet and put on Facebook can come back to haunt you*. Retrieved from The Montreal Gazatte: http://www.montrealgazette.com/business/Beware+social+media/5822233/story.html

Bernal, J. (2010). *Web 2.0 and Social Networking for the Enterprise.* Crawfordsville: IBM Press.

Berwaerts, P. (2011, December 28). *The Right to be Forgotten*. Retrieved from Business 2 Community: http://www.business2community.com/government-politics/the-right-to-be-forgotten-0111815

Booz Allen Hamilton . (2011, November 29). *Booz Allen Reports Top Ten Cyber Security Trends for Financial Services in 2012*. Retrieved from Booz Allen Hamilton: http://www.boozallen.com/media-center/press-releases/48399320/cyber-top-ten-2012

Boyd, E. B. (2011, January 31). *How Social Media Accelerated the Uprising in Egypt*. Retrieved from Fast Company: http://www.fastcompany.com/1722492/how-social-media-accelerated-the-uprising-in-egypt

Britt, B. S. (2012, January 06). *Copyright issues when using music in videos*. Retrieved from School Video News: http://www.school-video-news.com/index.php?option=com_content&view=article&id=306:copyright-issues-when-using-music-in-videos&catid=33:copyright&Itemid=51

Broder, J. F. (2006). *Risk Analysis and the Security Survey, 3rd Edition.* Burlington: Butterworth-Heinemann.

Carlisle, D. (2011, November 30). *Social Media Spoliation Hits Lawyer Hard*. Retrieved from ARMA International: http://www.arma.org/policy/policy/newswire/11-11-30/Social_Media_Spoliation_Hits_Lawyer_Hard.aspx

CBS News. (2011, February 6). *Did the Internet Kill Privacy?* Retrieved from CBS News: http://www.cbsnews.com/stories/2011/02/06/sunday/main7323148.shtml

Chavas, J.-P. (2004). *Risk Analysis in Theory and Practice.* San Diego: Academic Press.

Robert Shullich, rshullic@earthlink.net

Cowley, S. (2012, March 12). *LinkedIn is a hacker's dream tool*. Retrieved from CNN Money: http://money.cnn.com/2012/03/12/technology/linkedin-hackers/index.htm

Eastman, M. J. (2011). *A Survey of Social Media Issues Before the NLRB.* Washington, DC: NLRB.

eBIZ MBA. (2011, December 15). *Top 15 Most Popular Social Networking Sites - December 2011*. Retrieved from eBIZ MBA: http://www.ebizmba.com/articles/social-networking-websites

Elky, S. (2006, June 6). *An Introduction to Information System Risk*. Retrieved from Sans Institute Infosec Reading Room: http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204

Fair, L. (2011, June 23). *The Fair Credit Reporting Act & social media: What businesses should know*. Retrieved from FTC: http://business.ftc.gov/blog/2011/06/fair-credit-reporting-act-social-media-what-businesses-should-know

FINRA. (2012, January 8). *About FINRA*. Retrieved from FINRA: http://www.finra.org/AboutFINRA/

FINRA. (August 2011). *Notice 11-39: Social Media Websites and the Use of Personal Devices for Business Communications.* FINRA.

FINRA. (January 2010). *Notice 10-06: Social Media Web Sites - Guidance on Blogs and Social NetworkingWeb Sites.* FINRA.

FoxNews. (2011, December 06). *Facebook Flaw Means Anyone Can See Private Photos*. Retrieved from FoxNews.com: http://www.foxnews.com/scitech/2011/12/06/facebook-flaw-means-anyone-can-see-your-photos/

Friedman, E. (2010, September 29). *Victim of Secret Dorm Sex Tape Posts Facebook Goodbye, Jumps to His Death*. Retrieved from ABC News: http://abcnews.go.com/US/victim-secret-dorm-sex-tape-commits-suicide/story?id=11758716

Frosch, D. (2011, May 2). *Enforcing Copyrights Online, for a Profit*. Retrieved from New York Tomes: http://www.nytimes.com/2011/05/03/business/media/03righthaven.html?pagewanted=all

Gaudin, S. (2010a, May 4). *Half of social networkers post risky information, study finds*. Retrieved from Computerworld: http://www.computerworld.com/s/article/9176265/Half_of_social_networkers_post_risky_information_study_finds_

Gaudin, S. (2010b, June 28). *Social networks leak your information, Study says*. Retrieved from Computerworld: http://www.computerworld.com/s/article/9178648/Social_networks_leak_your_information_study_says

Gelb, A. R., Hall, E. N., & Collins, E. T. (2011, February 1). *Social Media: More Reasons to Pay Close Attention to What Your Employees Say and What Your Company Does About It*. Retrieved from National Law Review:

Robert Shullich, rshullic@earthlink.net

http://www.natlawreview.com/article/social-media-more-reasons-to-pay-close-attention-to-what-your-employees-say-and-what-your-co

Goodchild, J. (2010, February 3). *Social Media Risks: The Basics*. Retrieved from CSO Online: http://www.csoonline.com/article/529764/social-media-risks-the-basics

Goodman, J. D. (2011, August 11). *In British Riots, Social Media and Face Masks Are the Focus*. Retrieved from NY Times: http://thelede.blogs.nytimes.com/2011/08/11/social-media-and-facemasks-are-targets-after-british-riots/

Greene, T. C. (2000, February 14). *Internet security firm RSA's Web site hacked*. Retrieved from The Register: http://www.theregister.co.uk/2000/02/14/internet_security_firm_rsas_web/

Grover, J., & Goldberg, M. (2010, February 12). *Hacked E-mail Accounts Used to Scam Friends*. Retrieved from NBC: http://www.nbclosangeles.com/news/tech/Email-Scams-83600577.html

Hachman, M. (2011, October 19). *Long-Awaited Google+ Features Arriving Soon, Execs Say*. Retrieved from PC Magazine: http://www.pcmag.com/article2/0,2817,2395009,00.asp#fbid=PLmTThEpB67

Hardaker, M. (2011, January 17). *Third Largest County In The World Facebook*. Retrieved from Mountain Weekly News: http://mtnweekly.com/if-facebook-was-a-country-it-would-be-the-third-largest-in-the-world-11731

Hawthorne, N. (2004). *The Scarlet Letter.* Barnes & Noble Classics Series .

Helft, M. (2012, January 10). *Google's search revamp is all about social*. Retrieved from Fortune Tech: http://tech.fortune.cnn.com/2012/01/10/google-search-changes/

Herssner, K. M. (2009, January 23). *BlackBerry Force One Is Up to the Job*. Retrieved from ABC News: http://abcnews.go.com/Technology/President44/story?id=6712260&page=1

Huffington Post. (2011, November 8). *Jennifer O'Brien, New Jersey Teacher, Should Lose Job For Facebook Post*. Retrieved from Huffington Post: http://www.huffingtonpost.com/2011/11/09/jennifer-obrien-new-jerse_n_1083947.html

I Hate Starbucks. (n.d.). Retrieved from http://www.ihatestarbucks.com/.

Indeed. (n.d.). Retrieved from www.indeed.com.

ISACA. (2010). *Social Media: Business Benefit sand Security, Governance and Assurance Perspectives.* Rolling Meadows: ISACA.

Jaslow, R. (2011, September 09). *Patient privacy in spotlight after hospital records posted online*. Retrieved from CBS News: http://www.cbsnews.com/8301-504763_162-20104038-10391704.html

Knightley, P. (2010, March 12). *The History of the Honey Trap*. Retrieved from Foreign Policy: http://www.foreignpolicy.com/articles/2010/03/12/the_history_of_the_honey_trap?page=0,3

Robert Shullich, rshullic@earthlink.net

KnowBe4. (2011, May 9). *KnowBe4 Research Reveals Companies Vulnerable to Cybercrime* . Retrieved from KnowBe4: http://www.knowbe4.com/about-us/press-releases/knowbe4-research-reveals-companies-vulnerable-to-cybercrime/

Krebs, B. (2008, December 3). *Court Rules Against Teacher in MySpace 'Drunken Pirate' Case*. Retrieved from The Washington Post: http://voices.washingtonpost.com/securityfix/2008/12/court_rules_against_teacher_in.html

Krill, P. (2011, March 9). *Big Data mining: Who owns your social network data?* Retrieved from InfoWorld: http://www.infoworld.com/d/business-intelligence/big-data-mining-who-owns-your-social-network-data-746

LeMay, R. (2005, April 13). *Blog censorship gains support*. Retrieved from CNET News: http://news.cnet.com/Blog-censorship-gains-support/2100-1028_3-5670096.html

Li, S. (2011, January 25). *Insurers are scouring social media for evidence of fraud*. Retrieved from Los Angeles Times: http://articles.latimes.com/2011/jan/25/business/la-fi-facebook-evidence-20110125

Long, J. (2005). *Google Hacking for Penetrtion Testes.* Rockland, MA: Syngress.

Masnick, M. (2011, December 8). *RIAA Doesn't Apologize For Year-Long Blog Censorship;Just Stands By Its Claim That The Site Broke The Law*. Retrieved from Techdirt: http://www.techdirt.com/articles/20111208/12500917012/riaa-doesnt-apologize-year-long-blog-censorship-just-stands-its-claim-that-site-broke-law.shtml

Mayer-Schonberger, V. (2009). *Delete - The Virtue of Forgetting in the Digital Age.* Princeton: Princeton University Press.

McAfee. (2010). *2011 Threats Predictions.* Santa Clara: McAfee Labs.

McAfee, A. (2009, November 13). *Weighing Social Media's Risks*. Retrieved from Forbes: http://www.forbes.com/2009/11/13/social-media-enterprise-technology-cio-network-mcafee.html

McFadden, R. D. (2011, March 11). *Carnage on I-95 After Crash Rips Bus Apart*. Retrieved from NY Times: http://www.nytimes.com/2011/03/13/nyregion/13crash.html?pagewanted=all

Mcgahan, M. F. (2011, December 01). *EEOC cautions employers on using social media in hiring*. Retrieved from Diversity Central: http://www.diversitycentral.com/law/index.html

McMillan, R. (2010, November 13). *Researchers take down Koobface servers*. Retrieved from Computerworld: http://www.computerworld.com/s/article/9196398/Researchers_take_down_Koobface_servers

Merriam Webster. (2008). *Merriam-Webster's Collegiate Dictionary, 11th Edition.* Springfield: Merriam Webster.

Robert Shullich, rshullic@earthlink.net

Merrill, T., Latham, K., Santalesa, R., & Navetta, D. (April 2011). *Social Media: The Business Benefits May Be Enormous, But Can the Risks -- Reputational, Legal, Operational -- Be Mitigated?* ACE Group.

Meyer, E. B. (2011, July 13). *Tweet this! More employers now allow social networking at work*. Retrieved from The Employer Handbook: http://www.theemployerhandbook.com/2011/07/study-more-employees-allowed-t.html

Miller, R. (2009, June 29). *Microsoft to Open Two Massive Data Centers*. Retrieved from Data Center Knowledge: http://www.datacenterknowledge.com/archives/2009/06/29/microsoft-to-open-two-massive-data-centers/

Muncaster, P. (2011, January 27). *Hackers ran detailed reconnaissance on Google employees*. Retrieved from SC Magazine: http://www.scmagazine.com.au/News/165600,hackers-ran-detailed-reconnaissance-on-google-employees.aspx

Murphy, K. (2010, August 11). *Web Photos That Reveal Secrets, Like Where You Live*. Retrieved from New York Times: http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?pagewanted=all

Nairn, G. (2011, October 19). *Your Wall Has Ears*. Retrieved from Wall Street Journal: http://online.wsj.com/article/SB10001424052970204226204576600531532461052.html

NYC Health. (2011, October). *Letter Grading for Sanitary Inspections*. Retrieved from New York City Department Of Health and Mental Hygiene: http://www.nyc.gov/html/doh/downloads/pdf/rii/restaurant-grading-faq.pdf

Nyman, F. (2011, October 24). *Social Media Damage is High on Risk Managers' list of Concerns*. Retrieved from Insurance Insight: http://www.insuranceinsight.eu/insurance-insight/news/2119417/social-media-damage-risk-managers-list-concerns

Olson, P. (2011, May 2). *Man Inadvertently Live Tweets Osama Bin Laden Raid*. Retrieved from Forbes: http://www.forbes.com/sites/parmyolson/2011/05/02/man-inadvertently-live-tweets-osama-bin-laden-raid/

Ponemon Institute. (2011). *Global Survey on Social Media Risks.* Traverse City: Ponemon Institute, LLC.

PR News. (2010, September 13). *Social Media Guidelines: Command And Control or 'Let 'er Rip!'*. Retrieved from PR News: http://www.prnewsonline.com/news/Social-Media-Guidelines-Command-And-Control-or-Let-er-Rip!_14129.html

PRNewswire. (2009, August 6). *Only One in Three Companies Address Social Media Concerns*. Retrieved from PRNewswire: http://www.prnewswire.com/news-releases/only-one-in-three-companies-address-social-media-concerns-62171422.html

Ragan, S. (2009, December 09). *As Facebook pushes to protect the kids - what about the adults?* Retrieved from Tech Herald:

Robert Shullich, rshullic@earthlink.net

http://www.thetechherald.com/articles/As-Facebook-pushes-to-protect-the-kids-what-about-the-adults

Reardon, M. (2006, April 7). *Protective parents: Gold for cellular services?* Retrieved from CNET News: http://news.cnet.com/Protective-parents-Gold-for-cellular-services/2100-1039_3-6058756.html

Richmond, R. (2011, March 18). *RSA's Secure IDs Hacked; What to Do*. Retrieved from New York Times: http://gadgetwise.blogs.nytimes.com/2011/03/18/rsas-secure-ids-hacked-what-to-do/

Ripoff Report. (n.d.). Retrieved from www.ripoff.com.

Robert Half Technology. (2011, May 26). *Social Work? More Companies Permit Social Networking on the Job, Robert Half Technology Survey Reveals*. Retrieved from Robert Half Technologies: http://rht.mediaroom.com/2011SocialMediaPolicies

Rusli, E. (2010, October 24). *Firesheep In Wolves' Clothing: Extension Lets You Hack Into Twitter, Facebook Accounts Easily*. Retrieved from Techcrunch: http://techcrunch.com/2010/10/24/firesheep-in-wolves-clothing-app-lets-you-hack-into-twitter-facebook-accounts-easily/

Sachoff, M. (2010, July 12). *More Employees Visiting Social Networks At Work*. Retrieved from WebproNews: http://www.webpronews.com/more-employees-visiting-social-networks-at-work-2010-07

Sachoff, M. (2010, May 4). *Social Network Users Posting Too Much Personal Information*. Retrieved from WebProNews: http://www.webpronews.com/social-network-users-posting-too-much-personal-information-2010-05

Schneier, B. (2010, August 10). *A Revised Taxonomy of Social Networking Data*. Retrieved from Schneier on Security: http://www.schneier.com/blog/archives/2010/08/a_taxonomy_of_s_1.html

Scott, P. R., & Jacka, J. M. (2011). *Auditing Social Media - A Governance and Risk Guide.* Hoboken: Wiley.

SimplyHired. (n.d.). Retrieved from www.SimplyHired.com.

Slattery, B. (2008, December 5). *Facebook Virus Turns Your Computer into a Zombie*. Retrieved from PcWorld: http://www.pcworld.com/article/155017/facebook_virus_turns_your_computer_into_a_zombie.html

Solove, D. J. (2007). *The Future of Reputation - Gossip, Rumor, and Privacy on the Internet.* New Haven: Yale Press.

Sophos. (2011a). *Sophos Security threat report 2011.* Boston: Sophos.

Sophos. (2011b). *Sophos Security Threat Report - Mid-Year 2011.* Boston: Sophos.

Staff, P. (2010, June 9). *Private Investigators Powering Searches with Social Media*. Retrieved from PI Now: http://www.pinow.com/articles/358/private-investigators-powering-searches-with-social-media

Steel, E., & Fowler, G. A. (2010, October 18). *Facebook in Privacy Breach*. Retrieved from The wall Street Journal: http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html

Robert Shullich, rshullic@earthlink.net

Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). *Risk Management Guide for Information Technology Systems (SP800-30)*. Retrieved from NIST: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Sullivan, B. (2011a, March 10). *Study: Social media polarizes our privacy concerns*. Retrieved from MSNBC.COM: http://www.msnbc.msn.com/id/41995992/ns/technology_and_science/t/study-social-media-polarizes-our-privacy-concerns/

Sullivan, B. (2011b, May 24). *That famous space shuttle photo: When is sharing stealing?* Retrieved from Redtape MSNBC: http://redtape.msnbc.msn.com/_news/2011/05/23/6703177-that-famous-space-shuttle-photo-when-is-sharing-stealing

Sutter, J., & Carroll, J. (2009, February 5). *Fears of impostors increase on Facebook*. Retrieved from CNN: http://articles.cnn.com/2009-02-05/tech/facebook.impostors_1_facebook-spokesman-barry-schnitt-cnn-friends-track?_s=PM:TECH

Symantec. (2011, July 27). *Social media risks surveyed*. Retrieved from Continuity Central: http://www.continuitycentral.com/news05853.html

Thompson, J. T., Hertzberg, J., & Sullivan, M. (2011). *Social media and its associated risks.* Grant Thornton LLP.

Timm, C., & Perez, R. (2010). *Seven Deadliest Social Network Attacks.* Burlington: Syngress.

Vilches, J. (2010, December 23). *Preview Shortened URLs and Avoid Security*. Retrieved from Techspot Guides: http://www.techspot.com/guides/350-preview-shortened-urls/

Warren, S. D., & Brandeis, L. D. (1890, December 15). *The Right to Privacy*. Retrieved from Harvard Law Review: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

WayBack. (n.d.). Retrieved from www.archive.org.

Websense. (2011). *Social media security risks: The elephant in the room.* Santa Clara: Websense.

Whittaker, Z. (2011, December 7). *European data protection law proposals revealed*. Retrieved from ZDNet: http://www.zdnet.com/blog/london/european-data-protection-law-proposals-revealed/1365

Yoe, C. (2011). *Primer on Risk Analysis - Decision Making Under Uncertainty.* Boca Raton: CRC Press.

Zagat. (n.d.). Retrieved from http://www.zagat.com/.

Robert Shullich, rshullic@earthlink.net