Social networking and the risk to companies and institutions

Marc Langheinrich*a, Günter Karjothb

a University of Lugano, Switzerland
b IBM Research Zurich, Switzerland

Abstract

Social networks open up new business opportunities for customer acquisition and retention, facilitate knowledge transfer within the company, and can positively influence work climate. However, they can also quickly destroy a company image that took years to build, while the use of social networks at work not only risks a loss in productivity but may also undermine legal obligations. Eager networkers might also divulge company internals to competitors or the public at large. And last but not least, “friendships” open up completely new attack vectors for professional hackers, thus significantly increasing company exposure to online break-ins. This article briefly summarizes the opportunities and dangers that this development poses for business. This contribution is based on an earlier article by the same authors (in German) (Langheinrich and Karjoth, 2010).

1. Introduction

By the last count (July 2010), the popular online social networking site (SNS) Facebook featured not less than half a billion users (Ostrow, 2010) – that is a few million more than, say, the population of all 27 EU member states together. In the US alone, Facebook’s user base grew more than 350% in the last 24 months – from 27 million users in July 2008 to more than 125 million in July 2010 (Burcher, 2010), representing 40% of the country’s population.

While much has been written about the benefits and risks of SNSs for individuals (e.g., Bilge et al., 2009; Fogel and Nehamad, 2009; Boyd and Ellison, 2007), their widespread use also increasingly affects companies and public institutions, even though such “legal persons” hardly seem to be in need of finding friends. However, today’s SNSs have become a powerful tool for customer acquisition and retention, employee recruiting, for intra-company knowledge transfer, and for creating a positive workplace atmosphere.

At the same time, the ability of SNSs to quickly destroy a highly profitable brand image that took years to build up, using nothing more but a low-cost grassroots campaign, is equally powerful. Also, Facebook-enabled employees risk neglecting their actual work over extensive networking (as of April 2010, almost 7% of all corporate Internet traffic is said to have come from accessing Facebook pages (See http://www.network-box.com/node/533)), or unknowingly spilling company secrets to “friendly” competitors. Firing employees that are “friends” with their managers might risk lawsuits that stipulate the improper use of private information, while hacking the SNS accounts of management can significantly improve the success rate of phishing attacks. Should companies avoid or embrace SNSs?

2. Social networks and social selling

The future of advertising is personal. This not only means “personalized” in the sense that companies can prepare custom messages to individual customers, but also “personal” in the sense that product endorsements and tips come directly from friends, for friends.

Examples of this new type of advertising are the so-called “viral marketing “ campaigns on the Web: A company might leak some apparently unauthorized pictures,
videos, or specs of a soon-to-be released product to a well-known blog, from where the information quickly spreads by word of mouth around the entire world. Critics argue that Apple’s iPhone4 leak in April 2010 was a prime example of this, when the super secret prototype of its latest gadget was apparently lost by an employee, only to be found by the editor of a well-known technology blog (Phillips, 2010).

Companies such as Amazon, Netflix, and Tripadvisor have popularized an equally powerful marketing tool — in the case of Amazon it concerns books and videos, in the case of Tripadvisor hotels and restaurants — where customers write the reviews of the products they liked or disliked. This way, potential customers do not have to believe the hype of a marketing department but instead can rely on first-hand experiences by previous customers.

SNSs take this approach one step further: instead of receiving reviews and other information from unknown third parties, consumers receive product-related information (e.g., experience reports or even just buying decisions) from people they know, and whose tastes and preferences they are aware of, and which they potentially share.

Facebook’s “Beacon” program was a first (albeit failed) attempt at implementing such a “word-of-mouth” campaign tool in an SNS. As soon as a Facebook user would buy an item from a participating online shop (e.g., a book at Amazon), all of her Facebook friends would be told about this in the form of a status message: “Alice just bought ‘War and Peace’ at Amazon”. This allowed one to easily stay up to date about one’s friends’ shopping behaviors. Beacon ultimately failed, mostly due to its awkward market introduction: instead of offering Beacon as an optional service, its features were enabled by default across the entire user base, mostly without the knowledge of users. As a result, many secret presents bought at Amazon announced themselves via Facebook at their recipients, often days before the buyer would receive the actual shipment. Only 9 months after the much publicized introduction, Beacon was canceled in September 2007 after a landslide of negative press (Mccarthy, 2009).

Less than 3 years later, Facebook launched the “Like” button (April 2010) – practically Beacon 2.0, yet with an explicit “opt-in” behavior. A Web site operator can simply embed a pre-defined HTML string on its site in order to participate in Facebook’s so-called “OpenGraph”. This not only allows Web site visitors to feed information into Facebook, but also enables Web site operators to retrieve information about their visitors from Facebook. Visitors may now proclaim their sympathy with a company or a product simply by pressing the (prominently placed) “Like” button. This preference is then communicated not only to the visitor’s entire social network, but also to all companies participating in the Facebook advertising program. The popularity of a product or brand might soon be measured not only the “Google” way, i.e., using the number of links that point to its Web pages, but “up-close and personal” by counting the number of Facebook users who clicked on its “Like” button. What companies can afford to stay away from such powerful popularity tools?

Viral marketing is also entering new dimensions through the use of highly connected social networks. SNSs give viral marketing a spin similar to the “flash mobs” phenomenon, in which a large group of people previously unknown to each other spontaneously organize a meeting, typically with a theme that carries a Dadaistic connotation, using the Internet and SMS texting. With social networks, a viral marketing campaign can quickly and easily establish interest groups for newly launched products or upcoming events. By now, few commercial heavyweights can afford not to have a presence in these social networks: from the Volkswagen Golf to the Kit Kat chocolate bar, from U.S. President Obama to the product “Facebook” itself: all have established their dedicated presence in Facebook. By now, even places (e.g., “Times Square”) and activities (e.g., “Pillow Fighting”) can get their own Facebook pages, thus allowing people to “befriend” them.

While such product pages have a tremendous potential for not only cost effective but also extremely targeted and effective advertisement, they are much harder to control than traditional advertising channels and can thus quickly lose the control of their “creators”. Nestle learned this the hard way in March 2010: After someone posted a Greenpeace article to the Kit Kat Facebook group that strongly criticized Nestle for sourcing its palm oil from a company that routinely razes large areas of rainforest for harvesting it, boycott calls were quickly raised. As basically any Facebook user can become a member of a fan group, activists were quickly able to take over the group, and soon had transformed it from a tranquil community into an angry mob. The first stop for fans had become the first stop for critics. Nestle – as the group’s creator – further intensified the conflict by using its “admin rights” to delete critical posts. Even though Nestle claimed that the palm oil in Kit Kat did not come from the particular supplier in the Greenpeace article, Nestle soon had to back down and publicly pledge to only use environmentally friendly certified palm oil in the future (Tabacek, 2010).

Of course, critics can also create their own “fan” group instead of taking over an existing one — as in the case of the British television talent show X-Factor, an updated version of the hugely popular “Pop Idol”/”American Idol” TV format. In its native country UK, a well-oiled marketing machine had ensured that the X-Factor winner would also manage to have the best-selling Hit Single in the lucrative Christmas shopping season. To stop this recurring phenomenon, critics created a fan group in 2009 for the sole purpose of motivating enough “fans” to buy a different Single this Christmas. An indeed: by Christmas Day, their favored Indy song managed to surpass the X-Factor hit by a considerable margin of more than 50,000 sold copies. Again, a small band of activists had successfully beaten a huge and costly advertising campaign, simply by “connecting” with their friends.

Social networks as a viral marketing tool are thus a double-edged sword: they allow for an unprecedented dissemination of marketing messages at minimal cost, but they remain largely out of control, and can quickly turn into negative publicity. They effectively “level the ground” between marketers and consumer activists, who can now run worldwide campaigns virtually free of charge with the help of SNSs.

3. Social networks as a leadership tool

Social networks can not only improve communication with existing and potential customers, it can also positively affect the communication within an organization.
Even without an official adoption of Facebook by management, many employees probably already spend considerable amounts of company time to “quickly” check their profile and update their status while at work. A good example is the case of the city administration in Zurich, Switzerland. After their 24,000 employees had a combined daily load of seven million Facebook accesses per day, management decided to explicitly address the issue. Yet during a 3-month trial phase asking for voluntary self-restraint, no significant dip in those figures occurred, so IT services finally blocked all access to facebook.com (Gattiker, 2010). In the United States, almost 40% of all companies have already blocked access to social media of any kind (How Effective Are Corporate Social Media Policies?, 2010).

While unrestricted Web access has certainly become a regular perk that often positively contributes to a company’s work climate, the excessive use of SNSs quickly tests the limit of this instrument. With countless small updates and checks needed to properly tend to one’s social profile, such perks can quickly turn into first-rate time killers.

Instead of simply allowing or blocking SNS access, some companies explicitly use it as a leadership tool. Managers use SNSs to befrend their team members, thus creating a seemingly casual work atmosphere. Regular status updates within an SNS group may help to coordinate work and also create awareness about the activities of individual team members. Yet lawyers already warn that mixing with the rank and file in awareness about the activities of individual team members. Yet lawyers already warn that mixing with the rank and file in a rather conservative image can profit tremendously from viral channels of SNSs, i.e., as a potential employer for prospective recruits. In particular companies that have a rather conservative image can profit tremendously from such a use of SNS, as this helps to project a fresh and youthful image. A case in point is the French Catholic Church, which in 2010 started a new Facebook group for people with an interest in priesthood connecting them to actual priests for first-hand advice (King, 2010).

Companies can of course also advertise themselves on the viral channels of SNSs, i.e., as a potential employer for prospective recruits. In particular companies that have a rather conservative image can profit tremendously from such a use of SNS, as this helps to project a fresh and youthful image. A case in point is the French Catholic Church, which in 2010 started a new Facebook group for people with an interest in priesthood connecting them to actual priests for first-hand advice (King, 2010). Professional networks such as LinkedIn and Xing are specifically tailored to help companies locate candidates that offer certain skills and interests, and even to link potential employees to their former managers, thus allowing prospective employers to receive detailed information on prior job performances. Obviously, the same tools can also be used by headhunters to recruit the company’s existing employees for a competitor.

4. Recruitment and screening

In a study published December 2009, Microsoft surveyed more than 1200 recruiters about their use of networked media for recruitment (Research Shows Online Reputations Matter, 2009). While classical search engines were still used in the large majority of cases (78%), SNSs followed not far behind (63%), indicating that they have become an integral part of employee screening. Equally popular were SNS-influenced sites such as photo-sharing platforms (e.g., Flickr) with 59% and professional business networks such as LinkedIn or Xing (57%). Half a year earlier, a Harris Interactive study had found a rate of only 45% for the use of SNS in recruiting (Wortham, 2009).

Over the years, SNSs like Facebook have significantly expanded the amount of personal information that is accessible through the public profile of a person—in most cases without the profile owner being aware of this. Consequently, potential employers today can often have a detailed look at the interests and relationships of a potential employee, even without being “friend” with the candidate. In early 2010, Facebook for example changed group membership and preference information (e.g., interests such as books or movies) in the user profile from simple fields to a “connection”. While looking like a mere technicality, the change significantly expanded the amount of profile information that is now publicly accessible. In contrast to simple profile fields, connections are per definition visible to all users with a similar connection. Thus, all people who showed an interest in “Pillow Fighting” will now know who else likes pillow fighting, etc. This change already inspired activists to “hunt” for members connected to the “wrong” ideas and interests. Together with other activists they massively report those unwelcomed Facebook members as “spammers” with the aim to ban them, thereby exploiting Facebook’s “wisdom of the crowds”-based automated account shutdown feature (Hopkins, 2010).

Employers might be tempted to similarly exploit this information in order to find potential lay-off candidates. Yet as pointed out above, SNS information is difficult to use in labor related litigation. Ideally, employee activity on an SNS clearly violates published company rules, rather than just being an “unpleasant” act. Such a case was published in 2005, when Google fired a newly hired product manager after only 11 days: As the product manager had used his blog to spread internal company information, he was in clear violation of written company guidelines and thus the use of his SNS-related activity was easily admitted in the proceedings (Hansen, 2010).

5. Dangerous liaisons — employees in social networks

The participation of employees in SNSs may not only reduce their productive working time and allow headhunters to woo them away to a competitor, but it can also quickly and significantly complicate corporate security.

5.1. Statistical insights

Most companies do not publish detailed information on teams, their members, and their current projects. However, the above-mentioned implicit publication of connections in an SNS such as Facebook can easily provide outsiders with a detailed insight into the internal operational structure. A few years ago, Amazon.com had to quickly learn that companies were not amused about exposing employee information, however innocuous it might seem: when the online book seller decided to publish aggregated buying patterns (“purchase circles”) of its customers—broken down not only by countries and cities, but also by companies—it quickly had to disable this feature again.
due to protests from many large companies (Amazon modifies purchase circles following controversy, 1999). Social network platforms in turn often watch out that their own data collections cannot be automatically harvested on a large scale either (Scoble, 2008). Instead, the aggregated information is usually part of the social network’s marketing tools that it offers to its advertisers (See http://www.facebook.com/advertising/).

Even non-aggregated, individual profiles can already provide sensitive insights. If, e.g., a key account manager adds a client to the list of “friends”, this information would not only be of interest to competitors, but it might also potentially violate a customer confidentiality agreement. Even private chats between colleagues at the same company can spell trouble, as system errors might briefly expose even private conversations to a wider audience worldwide: when Facebook rolled out its new “preview my profile” feature on May 5, 2010, a glitch made both private chat records as well as pending friend requests temporary available to the public (Wortham, 2010).

5.2. Channel chatter

Also, the inherent human desire to communicate should never be underestimated. This all-too-human trait can quickly mislead employees who actively participate in social networks or social media to reveal – consciously or unconsciously – not only personal information but also company secrets. In Germany’s “Twitgate” scandal in 2009, news of the re-election of the German President Horst Köhler were secrets. In Germany’s “Twittergate” scandal in 2009, news of the re-election of the German President Horst Köhler were tweeted by an eager member of parliament some 15 min before the official result (Bryant, 2009). A slightly more serious breach occurred in March 2010, when the Israeli army had to call off a planned surprise attack in the West Bank after a soldier had bragged about his participation in the raid on his SNS profile (Mackey, 2010). SNSs and other participatory media (e.g., photo and video sharing sites) can also be used by frustrated employees to spread negative or even derogative comments about customers, thus significantly harming a company’s brand image (as in the case of Domino’s Pizza or Virgin Airlines (Fahmy, 2010)).

Even if employee postings and chat messages do not reach the wider public, questions remain about the legal status of the information distributed within a social network, especially if it concerns business intelligence. Knowing the specific terms and conditions of the SNS operator is a start, yet given that such policies are frequently changed (and often without notice), the risk of complete disclosure of such messages must be taken into account.

5.3. Spear phishing and other attacks

Not only chats and postings of employees are a source of concern, already the most basic employee profile data can help hackers to more easily penetrate a secured company network.

At the outset, hackers can use the personal information that employees use to register their SNS accounts (which many assume to be private, yet it often is, for the most part, made public) to authenticate themselves to poorly secured help desks: not only do profiles help with finding names and departments, some even feature a birth date and/or a company-internal phone number – information that is often accepted as a proof of identity over the phone.

Similarly, publicly available images may be used to create a false identity that allows a hacker to become “friends” with company employees, who may then unknowingly disclose internal information. A request for “friendship” that includes the right photo, the right department, and the right name might not create suspicion, in particular if there is no direct contact outside the social network (e.g., by claiming to be a colleague from a different company location). A 2009 report by Sophos, a security company, found that 46% of Facebook users would regularly confirm friendship requests from unknown people (Facebook, 2010).

To exploit this, a professional phishing attack might begin by exploring publicly available company groups, often set up by employees. Next, the hacker would join such a group using a fake identity, allowing him to gain access to all group member profiles. This would allow for the creation of a detailed list of employees and their departments, to be targeted in the second step of the attack. When performing the actual phishing, the hacker reserves a domain with a similar name as the target company and installs a Web page on it that offers some generic service (e.g., human resources, or corporate pension scheme) and which adheres to the company’s corporate design. The phishing email itself is then sent on a Sunday night to hide in the flood of messages that opens up on Monday morning. It apparently comes from a human resource colleague (whose name the hacker found in the SNS group) and it invites the employee to log into a newly created portal, using their “usual” username and password. Any login attempt, however, is rejected with a generic “under construction” message, which manages to avoid suspicion, while the username and password pairs collected will be immediately used for the actual attack on the corporate network.

Sending targeted emails to employees that properly take his or her mission and role within the corporate hierarchy into account is called “spear fishing”, since it avoids the blunt use of hundreds of thousands of random email addresses (as in traditional phishing) and instead focuses only on the most promising victims (Stasiukonis, 2010). Social networks and professional networks thus play a significant role in this attack, as they can help hackers to greatly increase the authenticity of those fake emails using the background knowledge gained from an SNS (Martinez-Cabrera, 2010). Even more powerful attacks can be launched if a hacker manages to break into the existing social network account of a company manager (ironically, this happens even to Facebook board members (McCarthy, 2010)); by sending messages directly from a real account, hundreds of employees may quickly fall into such a phishing trap. Breaking into such SNS accounts is often simplified by the trivial security questions that many service provider force their users to set up, in order to ease lost password recovery. A prime example of this could be witnessed in the 2008 presidential election race in the US: a college student was able to take over the Yahoo! email account of Sarah Palin, the Republican presidential candidate, by simply answering the account’s security question “Where did you meet your spouse?” The answer was only a quick Internet search away: at “Wasilla High” (Zetter, 2010).

Guarding against such phishing attacks is complicated by the increasing number of mobile devices (e.g., laptops and
smartphones) that employees use to access company services while on the go. Stored password on such devices become a nightmare for corporate security should the devices be lost by the employee. The identification of fake URLs in such phishing attacks is also difficult, given the severely restricted display lengths of most smartphone browsers.

5.4. Archiving requirements and online chats

Last but not least, SNSs and other social media such as Twitter can also have a profound effect on corporate governance. In both regulated industries and in the public sector, all employee communication must typically be archived. While corporate email solutions typically support such requirements, the use of social media for communication is often in direct violation of these regulations. A prominent example was the Google “Buzz” scandal of April 2010, when Andrew McLaughlin, former Google employee and by then Deputy Chief Technology Officer for the US President, was bitten by a bug in Google’s newly launched service that involuntarily would expose one’s most frequent Gmail contacts to the public. In McLaughlin’s case, this not only included old colleagues at Google (which triggered questions about his friendly relationships with industry), but also listed many White House colleagues. With the high archival standards imposed by the Presidential Records Act, the potential use of his private email account for White House business would have been a serious violation (Froomkin, 2010). As of today, record management and digital archiving of information for SNS do not yet exist.

6. Conclusions

With the many advantages of embracing SNS and other social media communication channels, companies need to carefully evaluate not only the opportunities of such a move, but also face the risks. In 2007, ENISA – the European Network and Information Security Agency – published 19 recommendations for operators and users of social networks (Hogben, 2008). Today, similar recommendations exist for public authorities, for example those set up by the British government to improve administrative activities in social media (Taylor-Smith and Lindner, 2010). The most important issue is certainly the proper training of staff, as well as a thorough review and assessment of the legal implications. Having an official company policy about the use of social networks is an essential step to help employees use these kinds of services productively and safely. However, according to a February 2010 survey by Manpower, an employment agency, only about 11% of European companies had set up such a policy (Few companies have policy for employee use of social networks, 2010).

From a technology perspective, corporate IT needs to ensure that employee profiles use appropriate privacy settings, and that phishing attacks and other suspicious behavior can be automatically detected and/or easily reported. Operators of SNS should also better address the needs of businesses, ranging from offering more stable terms and conditions to providing stronger authentication mechanisms and proper access control tools. This might prevent future news about endemic user profile thefts (Heron, 2010).

References


Amazon+Modifies+Purchase+Circles+Following+Controversy.htm August 27, 1999.


