Understanding Social Media Risks and Considerations

By: Ken Foster, KMBL Security

6/20/2012

In the environment I work in, management has embraced the concept of Social Networking as a mechanism to share key organizational events, information, provide positive brand recognition, address customer issues, and make the senior manage and their activities more accessible to the rank and file. These are all admirable goals. However, the introduction of wide-spread social media use also introduces risks that if not properly understood and appropriately understood, could result in embarrassing disclosures and potential regulatory issues. The content of this paper is intended to highlight areas for further consideration with regards to how organizations and their employees operate in these environments.

For the purposes of this discussion, I will use the GFI Social Networking and Security Risks white paper as a common reference (Dinerman, 2012). This reference is by no means an inclusive resource. Let's begin by considering the social networking goals of fictitious organizational and their potential associated risks:

Goal	Intended Purpose	Mechanism	Associated Risk
Employee Engagement	Connect with current employees	Facebook	Site must be set as a "Page" not a profile in order to effectively manage content
Critical Communications	Distribute critical information to employee-base	Twitter	Is sent plain-text, readable by anyone who cares to try! Represents a security risk. Provides for re-tweeting to unintended persons.
Public Relations	Connect with interested / concerned 3rd parties	Facebook	People tend to rage more often in online environments that in person. This presents a risk for negative communications appearing on publically viewed pages not constantly monitored.
Positive Imaging	Produce and distribute positive media coverage of activities	Facebook Twitter	Broadcasting of stories like any other media can be misquoted, taken out of context, and repurposed as negative imaging, requiring correction and crisis management efforts
Group / Team / internal Organization Collaboration	Provides easy, mobile access to calendars, events and activities through mobile devices and from home	Facebook	A lack of organizational monitoring can allow for privacy information to be improperly stored, sensitive employee identity information leaked, provides potential for operational event knowledge to external personnel, places employees at risk

Table 1. Fictitious Organization – Goals for Social Media Use

So I have listed 5 reasonable organizational goals and potential impacts. So does this mean I am against Social Networking? Clearly I am not since you most likely found the link to this article on one of my social networking sites. What I am against? My concerns is the inadequate understanding related to the opening of social network usage to all employees without first providing the appropriate training and implementation of policies, roles, and responsibilities. This paper is designed to open a dialog for management to consider what is appropriate use; when it is permissible; using what organizational resources; their frequency of use; and what preemptive steps are needed to reduce organizational risks when using these types of resources?

Training: We do not allow new employees to jump on a forklift and start driving throughout the warehouse until they are properly trained. Why not? This type of behavior is risky because they lack the general understanding necessary to operate the tool safely! So why then would we allow employees to use social networking sites on organizational time, with organization resources, until they are properly trained on how to operate in this environment safely? What you post at home on your personal account and what is posted when you are representing the organization are not always compatible. Do we provide guidance on how to separate the two and when risky behavior can have negative impacts? We should train our employees on how to use social media, what happens to a post once it's sent, and how cyber stalkers use this medium. This is basic employee safety training. This training should be extended at some point to take home materials for their families, who play a role in our employees' safety and security. Mr. Dinerman provides some interesting examples of risk related to untrained employee personal information leaks on pages 3-5 of his paper (Dinerman, 2012).

Policies: You cannot expect an employee to conform to a guideline or policy if it's not clearly addressed in writing, adequately distributed, accessible, and generally known within the organization. Policies are essential tools so that management can communicate their expectations with regards to professional conduct, issue resolution, time management, and information security. Allowing employees access to social networking sites without a clearly formulated social networking policy is a precursor for disaster. Let's view an example:

> *Bob, a 10 year tenured employee posts on his personal Facebook page, "I heard a rumor that we might be shutting down the 2nd shift; man I feel sorry for those people."*

Bob is discussing a genuine concern for other employees of the organization. It doesn't really matter if Bob is right or not, the firestorm is about to begin! This post is most likely distributed within seconds using Bob's friend's linkage to other employees, who then respond and re-post the rumor, causing exponential exposure. This can cause workplace stress, premature employee loss, safety risks to co-workers, and negative company press. Is Bob within his rights to post this? Well, that depends on the organizational policy? Without a non-organizational sensitive information disclosure guideline, Bob is free to exercise his freedom to post as he wishes without the possibility of Human Resources (HR) repercussions. However, if a clearly worded statement regarding the release of internal, organizationally sensitive information is only authorized by appointed organizational officials, then HR may have grounds to take administrative action against the employee. Mr. Dinerman addresses the needs for this clearity

through a well-defined Acceptable Use Policies (AUP) on page 5 of his paper (Dinerman, 2012). If our employee's understand their roles and the impacts of violating the policies for posting such sensitive information in a public forum, this might dissuade them from doing so. Is it a guarantee; absolutely not! However, without such policies in place, it is guaranteed that organizationally, you will have no recourse when it occurs. When forming your policies with regards to social networking, it's critical you include representation from management, rank and file employees, legal, and public relations. The resulting guidance should be easily understood, reasonable, actionable, and legally sound.

Roles and Responsibilities: Organization membership is a team sport. Everyone is on the team and only by everyone doing their part can the organization be successful. So how does this apply to social media? First, we need to establish roles within the organization.

Official Representatives: Who is responsible for posting on behalf of the organization (an authorized represented)? Have those representatives receive the appropriate training? Is there a mentorship mechanism for addressing unusual or offensive materials posted by employees or the public? Is it well understood?

Content Reviewers: Can content creators directly post to these public forums or must the content be reviewed for message consistence and accuracy? Consider running your online presence like your print presence. Having a second set of eyes on a proof can catch simple and unintentional mistakes.

Brand Management Monitors: Your organizations positive reputation took significant effort to build, but only seconds to destroy! Brand Managers are the individuals tasked with performing broad searches of the internet to see what others are posting about your organization. In many respects, this is both a customer service role as well as a public relations function. If slanderous, inaccurate, or otherwise negative posts are occurring, organizationally you have no mechanism to understand why or potentially address inaccuracies.

Policy Enforcement: Who is responsible for reviewing reported policy violations? What protections are the accused employees afforded? Is a policy of graduated offences well defined? Are accidental, unintentional, low risk disclosure or policy violations addressed as learning opportunities? Are employees encouraged to self-disclose accidental violations with no or minimized HR involvement? When is HR and Legal engaged in the process? Is law enforcement engagement recommended or authorized? These are all very complicated issues that must be clearly documented in internal policies (from a general sense) and fully articulated from an internet operating procedure perspective. Be prepared for legal challenges for negative personnel actions by ensuring the Legal and HR team provide input and review prior to implementation. Organizationally, you are required to let an employee know about policies related to acceptable conduct. What level of evidence collection and handling is required? Who established the chain of custody and who and how is the evidence secured? You're not required to document the tactics and techniques used to monitor and enforce the policy; only notify them that monitoring and compliance mechanisms exist.

User Responsibilities: By far the organizations single most effective mechanism to monitor activity is its employees. It's important our organizational users understand what is considered acceptable and what is not. They should be encouraged to self-monitor their activities and provide mentorship to others who are not following the guidelines. When an offense is identified, they should be encouraged to report it to the Policy Enforcement staff. Employees should feel comfortable in the knowledge that honest mistakes will be addressed as such and failing to identify these accidents are not in their or the organizations best interest.

Only through the careful consideration of these issues, can an organization appropriately address social networking use, acceptable content, risk reduction strategies, and internal processes. I hope this paper has provided you better awareness of these areas and generates an active internal discussion of your current processes, procedures, training, and responses related to this complex issue.

Works Cited

Dinerman, B. (2012, June 20). *Social Networking and Security Risks*. Retrieved from GFI.com: http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf