

Case Study: Social Media – Assessment, Risks and Techniques (SM-ART) Applied Discovery In Partnership With Sensei Enterprises

Virginia P. Henschel, Esq.

APPLIED DISCOVERY

Sharon Nelson, Esq.
and John Simek

SENSEI ENTERPRISES

Background And Risk

A corporation with 5,000 employees with several field offices had recently become aware of the perils of social media. For years it had authorized blogs and a Facebook page – thankfully none had presented any problems. In the last year, though, several issues came to the corporation's attention:

- **Disclosure of confidential business information.** One of its employees had a personal blog containing references to the corporation's research and development. One product, in particular, was expected to hit the marketplace with a bang, and the information being leaked was giving information to competitors. Another employee brought the blog to management's attention.

- **Reduced employee productivity.** Several supervisors came to management worried about the loss of employee productivity because employees seemed to be spending a lot of time on social media sites.

- **Lack of uniform practices throughout the organization.** Individual units of the corporation developed ad hoc social media directives but there was no uniform social media policy. Some units encouraged social media use on behalf of the corporation, yet others forbade it.

- **Public exposure of negative remarks by current employees.** One employee had a personal Facebook account and was posting derogatory remarks about her colleagues and supervisors. The corporation wasn't sure whether these posts were being made at home or at work, but it was concerned about legal ramifications.

- **Potentially damaging remarks about competitors.** Another employee in a business development unit who had a corporation-sanctioned Twitter account had posted several tweets disparaging competitors. The corporation was concerned about controlling this sort of activity.

- **Damaging remarks by former employee.** One disgruntled former employee left the corporation and used corporate Facebook credentials to post an angry rant against his former employer. Though the credentials were revoked, the corporation realized it had no procedures in place to remove social media credentials when employees leave its employ.

Management realized it had risk management issues involving social media, and also realized that it needed to be educated about social media, its potential threats and how to effectively manage social media. Having heard about the SM-ART program, the corporation called to discuss its concerns, its goals for having a social media assessment done and to ask questions about customizing

Virginia P. Henschel is Vice President of e-discovery affairs for Applied Discovery, a worldwide electronic discovery leader offering multinational collection, processing, review, and production services for law firms, corporations, and government organizations engaged in audits, investigations, and litigation. www.AppliedDiscovery.com. Sharon Nelson is President and John Simek is Vice President of Sensei Enterprises, a computer forensics and information technology company in Fairfax, Virginia.

the assessment and reporting for its specific needs.

Plan And Execution

Once the client and SM-ART agreed to a customized proposal and scope of work, two SM-ART representatives (a lawyer and a legal technologist) arranged a two-day formal meeting at the corporate headquarters.

Day One:

- The process started with a kick-off meeting with representatives from management, legal, business development, IT, marketing and human resources which included introductions, a presentation from the SM-ART representatives on the current state of social media as it impacts business and some of the legal implications.

- The team identified known issues and discussed further issues that might be uncovered during the assessment.

- Key employees were identified as possibly misusing social media and potentially exposing the corporation to liability. It was agreed that their machines would be forensically imaged after hours to allow for a full forensics examination of their computer activities, including deleted data. In several cases, it was also necessary to get a forensic image of corporate provided laptops.

- Together with the SM-ART team, they identified specific steps to be taken during the assessment, including installing an appliance on the network to confidentially monitor social media use for a period of two weeks.

- Based on the presentation and discussions with the SM-ART representatives, each element of the scope of work in the proposal was fleshed out and a project plan was created.

- The lawyer began conducting individual interviews of the SM-ART team to understand each individual's job function as it related to social media.

Day Two:

- Interviews were conducted with a cross section of employees discussing their use of social media. Key employees had been identified by the SM-ART team for interviews and others were randomly selected. From the interviews, the SM-ART representatives learned several important things:

- Some employees acknowledged that, in those business units which prohibited the use of social media, they evaded the policy by using their smartphones.

- Several employees mentioned social media activities of other employees which they thought exposed the corporation to risk.

- Some employees expressed anger at prohibitions placed on social media use by their business units.

- Fifty percent of those interviewed had no idea whether a social media policy existed. One hundred percent thought there should be a policy. Ninety percent thought it should be a "sensible" policy which allowed incidental use of social media on the corporate network, subject to "common sense" provisions.

- Those who used social media on behalf of the corporation expressed a keen sense of independence about what they did. It was evident an organized monitoring process had not been established or implemented, nor were they receptive to any supervision.

- The vast majority of those interviewed personally participated in Facebook, with some participating in Twitter and LinkedIn, and a few participating in other forms of social media. Several acknowledged that they had discussed their employer

occasionally but they were reticent about specifics.

- The legal technologist monitored the status of the installed appliance and provided training in managing the appliance, as well as in how to disengage the appliance after the two-week monitoring period and to securely send the data for analysis.

At the conclusion of the second day, the SM-ART representatives met briefly with previously designated representatives of the SM-ART team to report on its preliminary findings.

Results

Once back in their offices, the SM-ART representatives documented their onsite findings and then awaited the expiration of the two-week social media monitoring. Once the data had been received, they began their analysis.

Key Findings

1. A small but significant number of employees were spending excessive amounts of time on social media sites, seriously curtailing their productivity. Some were actually involved in third party social media games such as Farmville and Mafia Wars, which present additional security concerns.

2. More than 60 percent of employees (in business units where it was permitted) were indeed using social media during work hours. Most of that use did appear to be problematic.

3. Where business units had banned social media activity, it was clear that it was going on anyway, as employees from those units were posting during business hours. As the network did not reflect such usage and yet the posting was done during work hours, it was fairly certain that employees were using smartphones to avoid the prohibition.

4. The examination of those machines which had been forensically imaged revealed that one employee was actively sending out via web-based mail proprietary data to a competitor who had promised him employment. The clue to this activity came when the competitor was discovered on a Facebook friend list (this had been reported by a corporate employee). Searching on the competitor's name revealed the leak.

5. One employee was posting sexual material and photos of himself clearly intoxicated on his personal Facebook page.

6. Some of the key employees who had been identified for closer examination of their social networking activities proved to be quite problematic.

- a. One was seriously disparaging competitors.

- b. Another was sharing confidential corporate data on a sporadic basis.

- c. Several employees were posting negative remarks about their employer or their colleagues, much of it posted while on the company network.

- d. Some of the sanctioned social media activity taken on behalf of the corporation was ill-advised, at the very least. The need for designated personnel to review this kind of activity was clear.

- e. The employee who was terminated continued to use his credentials to make postings on the corporate Facebook page until it was reported and the credentials were terminated.

- f. One piece of well-documented malware which spreads through Facebook was identified as being on the corporate network.

- g. Multiple YouTube videos filmed by employees were discovered, mentioning it by name and reflecting poorly on the corporation.

SM-ART Team Recommendations

There were a great many recommendations and action items in the final report, including the following:

1. **Development of a uniform social media policy.** The SM-ART representatives submitted a proposed uniform social media policy based on the goals and objectives identified in the kick-off meeting. In accordance with that meeting, incidental use of social media would be allowed with guidelines governing such usage. Employees were to be advised that the employer had the right to monitor their social media activities and a signed statement of the policy would be placed in their personnel files.

2. **Identification of a new social media management position.** It was clear that someone needed to monitor, and perhaps pre-authorize any social media postings officially done on behalf of the corporation. That same position could be used to randomly audit social media usage, identifying flash points by searching on the corporation's name on the major social media sites real-time, potentially acquiring software or hardware to assist in this effort.

3. **Creation of a social media incident response team.** Should an incident happen, a team would be pre-identified to move in and do PR damage control and manage liability risk. It has often been shown that a prompt social media response by an affected corporation can seriously mitigate reputation damage.

4. **Development of an employee termination provision specific to social media.** The SM-ART representatives submitted sample language for management's consideration.

5. **Establish closer coordination with IT security.** Discuss the potential malware threats with IT and implement the most current hardware and software to protect against such threats.

6. **Address employee violations.** Several of the employees whose social media behavior was problematic needed to be terminated (particularly the employee who seemed to be providing confidential information to a competitor in anticipation of securing a job) or subjected to internal discipline.

7. **Set up a training program.** Create and conduct annual training sessions for all employees on the proper and safe use of social media, reiterating the corporation's social media policy and underscoring risk management.

After submission of the report, SM-ART representatives made themselves available for a two-hour telephone conference with the corporation's SM-ART team to answer questions and to develop an action plan based on the recommendations. The corporation expanded the scope of work to include an onsite visit by the SM-ART representatives to present the recommendations. Management believed that these changes, when presented by independent consultants, might have more credibility and encourage buy-in among the various business units. This visit included a presentation similar to that given at the kickoff meeting, but customized to reflect the data gathered from the onsite audit and focusing on how recommendations were developed and best practices for implementing the recommendations. The corporation largely accepted the policy recommendations and believed it could fine tune the language suggested by the SM-ART representatives, reserving the possibility that they might once again turn to the representatives if further social media issues arose.

To learn more about how the SM-ART service can help your organization assess, mitigate and manage social media risk, request a free consultation by email at smart@applieddiscovery.com.