

## **IT's Role in Social Business**

**By Seth Robinson, Director, Technology Analysis, CompTIA**

When it comes to utilizing social media for business purposes, the majority of the responsibility falls to the marketing or brand management staff. But, would you believe there is a proactive role that resides with the IT team? In order to create and maintain a comprehensive social strategy that meets business objectives, the IT department should be involved in everything from shaping company policy and assessing infrastructure capabilities to protecting company data.

### **Take a Lead Role in Building Policy**

With a company's initial foray into the social space comes the quick realization that the social presence requires a steady stream of input and that the lines between business use and personal use for many employees is blurry. To map out corporate objectives and describe appropriate conduct in a social environment, formal social policies should be put in place.

CompTIA's research study on social business finds that only 30 percent of companies already have a social policy, with another 34 percent planning on building such a policy. Among these companies, the IT department is the most likely to be involved with policy creation. Although the IT department is not typically seen as the owner of social activity, the experience with building policy regarding employee use of technology is easily translated into social environments. IT leaders should look for opportunities to help shape the company's mindset and objectives for social strategies.

### **Help Secure Social Activity**

The use of social media opens another avenue for security breaches within a company. In CompTIA's study, 25 percent of companies report that they have definitely had a security incident involving social technology, and another 21 percent believe that they have likely had a security incident. These incidents may be attacks from the outside, such as a user clicking on a link in a social site that leads to malware, or they may be an internal issue, such as an employee on a social site sharing data that was not meant for public consumption.

The typical response to a security incident is education. Fifty-eight percent of companies who believed they had a security incident educated employees on appropriate behavior in a social environment. Just as IT teams have experience in building policy describing how employees interact with technology, they also have experience with protecting employees and corporate interests in a technical environment. In addition to extending their leadership with educational offerings, IT departments can implement tools that may help monitor data, such as Data Loss Prevention (DLP) tools.

### **Analyze the Social Stream**

The data created through social activities produces two challenges. There are vast quantities of data, and that data is unstructured, making it difficult to collect in traditional databases. However, analysis of

this data is critical for a corporation, since it can contain insights based on popular opinion of a company's brand, offerings or policies.

Social analytics starts with listening – simple monitoring of streams through RSS or search capabilities of dashboards such as Hootsuite or Tweetdeck. These dashboards can also be used to manage corporate accounts, which is especially helpful when there are multiple accounts spread across various sites. Many of these tools and techniques are readily available to end users, but IT teams should still be aware of what is being used and assist with any initial setup or training.

More advanced analytics require specialized software. At this stage, an IT team will more naturally be involved, evaluating tools to ensure that increased investment will result in returns to the business. These tools can connect to other business systems, such as CRM, making integration and feedback important tasks for the IT team. Best practices in social analytics are emerging as this trend gains momentum, and the success stories in this space will be a large part of defining the ROI of social endeavors.

### **Build the Necessary Infrastructure**

The most commonly considered components of a social environment are the actual social layer (comprised of the individuals in the environment and the systems which connect them) and the application layer (comprised of tools such as social analytics that provide added value on top of the social layer). However, the underlying infrastructure supporting social environments must also be considered.

The large quantities of data dictate sizable storage solutions and robust networks, and the unpredictable nature of traffic drives a need for flexibility and dynamic load balancing. These qualities are hallmarks of cloud systems, so IT departments that are implementing social systems should consider cloud options when assessing their infrastructure capabilities.

By inserting themselves and helping to drive actions at all layers of a social initiative, an IT team can become a critical part of a company's overall social strategy. This type of proactive behavior is becoming increasingly important, not only for social business, but also for the general perception of IT as an integral part of achieving business objectives. CompTIA members have full access to additional social business information as well as a plethora of business resources at [www.comptia.org](http://www.comptia.org).