

Clash of Security and Social Network Marketing

Crystal Craven
Xcentic, Sept 20, 2010



Information Security Gurus and Marketing Professionals are often at odds with each other in the business realm. Marketing used to primarily be a print and face to face business function but thanks to the over-haul of standard marketing strategies, marketing has grown new roots on the web and has found itself buried deep within social networking sites like LinkedIn, Facebook and Twitter.

Michael Brooks, Publisher and Creator of the South Magazine states, "It is not a case of whether we will use them [social media sites]; it is how extensively we will and how much time we will invest into each. We look forward to these social medias developing further in order to make this type of outreach more of a science."

The need for businesses to have an online footprint is critical to reach the masses in today's competitive environment, but the potential loss of client data and the security threats it poses to your network are daunting. When the request for access to these social networking sites stem from an authentic business need, where do companies draw the line between marketing savvy and data security?

How do we, the paranoid Information Security folks, establish reasonable rules and boundaries? It seems that everyone within a company- managers and subordinates alike- have multiple social networking accounts. What prevention methods will be used to ensure our company or client's data isn't compromised? Who is going to monitor our company's Facebook account for appropriate business content while assuring client anonymity?

With network security always on the forefront of my mind, my initial thought was to shut it all down, block the popular social networking sites while on our domain. Why allow users to put our network at a higher risk of exposure to phishing attempts, spam and drive-byes from various extracurricular website activities? What happens when your users are home, on their personal computers, posting what they had for breakfast and griping about the daily grind at the office?

My suggestion is this: assess what level of risk your firm is willing to accept when using social media as a marketing tool, and establish a firm-wide policy on social networking. Outline the consequences of non-compliance and then enforce it. This won't be a one size fits all scenario. Be aware that staff at all levels are diving head first into these sites with little knowledge of the threats that await them. Educate your users; even your most well-seasoned executive probably has a Facebook account that is potentially exposed. Encourage users to err on the side of caution when posting personal information and data that might reveal confidential client or company information. Employers should clearly identify what information is to be kept undisclosed or confidential.

Finding the acceptable level of risk that still allows participation in the burgeoning growth of social networking in the business realm is the key to a symbiotic relationship between your Paranoid Information Security Staff and your Go Get 'Em Marketers.