

10 Things Every CEO and Managing Partners Should Know About Social Media

The following list of 10 was reported in the article [10 Ways IT Managers Can Deal with Social Media](#). It is essential that every Managing Partner and CEO read it as well, because they are the ones making decisions as they relate to social media. Please pass this on to the decisions makers, it provides some essential insights.

1. Be logical

Although it's easy to fear social networks, the reality is, most social networks don't pose the kind of security threats Windows does. Furthermore, most social networks don't pose the kind of threat e-mail phishing scams do. Is there are a danger? Of course. But it's not the biggest danger IT managers need to face.

2. Remember social networks have value

Social networks have some real value. Companies who give employees access to them can use employee profiles to promote their business. Happy employees will talk about their employers in a good light. It makes the company look good. And it might eventually bring in better talent.

3. Social networks are promotional tools

Having employees using social networks is a great way to promote business products or services. Think of social networks more as a public relations arm, rather than a security hole. Are there threats? Of course. But IT managers might just find that the benefits of promotion far outweigh the security issues that might arise.

4. Blocking only makes it worse

As Sophos pointed out in its study, blocking social networks is a bad practice. It only makes employees want to find ways to access their profiles through other means that have a higher likelihood of causing security issues in the enterprise. They will search for anonymizers. They will look for holes in security. And in the process, they might find some real trouble on the Web.

5. Education is important

Security software and hardware mean nothing without education. If employees don't know what they're doing or they don't know what to look for as issues arise, the company will have a higher likelihood of being affected. IT managers need to tell employees what to look out for. When they hear about security outbreaks on a network, they should alert employees. It's about being proactive.

6. Corporate policies work

Just allowing employees to access their social networks isn't enough. IT managers need

to develop a corporate policy governing access to the sites. It should include some basic information on using social networks. It should also remind employees not to divulge sensitive information at any point while being social. It might seem rather simple, but it could help keep corporate data safe.

7. Block the fringe

It might sound counter-intuitive, but IT managers should be blocking “fringe” social networks. Facebook, MySpace, Twitter, Bebo and FriendFeed are just fine. But don’t allow employees to access social networks that have a limited community. They tend to not be as regulated nearly as well as popular social networks and they could cause trouble for the company. And most employees probably won’t notice anyway.

8. Be open

Although it might be a pain to have to deal with every little employee issue, IT managers should be willing to have an open door policy with employees who want advice or answers to social networking questions. Do they want to know if they should open a file sent to them? Do they have questions about their privacy settings? If so, answer them. IT managers are the experts in that field—employees are not.

9. Be educated

In order to answer those questions, IT managers need to be educated on social networks. Don’t just use them once a week, get involved with their growth. Read popular Web 2.0 blogs to stay up on the latest news. Know when new updates launch. Have a real understanding of all the features. It will make it easier to address issues.

10. Go social

What better way for IT managers to truly embrace social networking in the enterprise than to join networks themselves? Become part of the community. Understand the employees’ passions. It could mean the difference between safety and danger.

Don’t try and build a fence around social media within your company. Your employees will try and find a way out, and you might not like the results. Use social media deliberately, that will give your firm or business the best chance of success.