Is Social Media Secure?
Is My Company Safe in Social Media?
Is Our Intellectual Property at Risk?
Is Social Media Too Risky?
What Do We Need To Do?

Answers to Frequently Asked Questions about Privacy and Social Media Security from two cybersecurity and data protection authorities.

Two local companies that help protect confidential personal and business information from unauthorized disclosure offer their experiences with Information Security in Social Media. Global Velocity is a St. Louis company that makes uniquely powerful network cybersecurity and content monitoring solutions. Redpoint Privacy Advisors is a St. Louis company that designs and implements information security awareness policies and programs for businesses and employees.

Is Social Media Secure?

Social Media is security agnostic. Social Media doesn't care about your security. It can be secure if you, your company, and your employees take measures to be private and secure. Otherwise, it is an inherently risky practice if there are not sufficient safeguards.

What kinds of privacy and security risks are there for companies using or getting into Social Media?

The most prominent risks to businesses due to Social Media right now are :

- An increased possibility of an intrusion into company networks;
- The theft or public disclosure of company trade secrets or intellectual property;
- Unauthorized access to the "personal" information of your clients and employees;
- Reduced competitive advantage based on information published via Social Media.

How does Social Media increase the danger of an unauthorized intrusion into company networks, files, and confidential business information?

Compared to conventional e-mail-based scams, social media-based attacks are potentially more clever and devastating. With company email, you could reign in the problem by controlling that email utility. With the exploding personal use of Social Media by individuals, companies are not as able to easily control the Social Media utility and protect the users from phishing or social engineering.

What happens in a typical Social Media-based attack that can gain access to an organization's network?

First, the hackers will target specific businesses that are likely to have valuable sets of information. Then, a cybercriminal can start to identify likely company representatives or employees by building an electronic dossier from FACEBOOK, LINKEDIN, TWITTER, and others. With this information about a company and its employees, the hackers can strategically attack them based on really solid personal information at both home and work.

What are the costs or repercussions of a data security incident?

In 2010, the average organizational total cost of a single data breach incident was $7.2 million.

For many of these business assets, the entire value of the company derives from their proprietary or confidential materials. If those potentially priceless intellectual property assets get into the wrong hands, the damage can be truly devastating to the company and endanger future operation of the company.

Most Businesses Believe that a Data Security Breach Wont Happen to Them. Is that Reasonable?

A recent report found that 88% of the organizations that it surveyed had at least one data security breach incident. So, no, it is probably not reasonable.

What are some examples of Best Practices in Social Media security? What are other companies doing?

We all agree that current "best practices" for Social Media Security involve a combination of administrative practices with technical safeguards. That means adopting a Social Media Strategy with Policies or Procedures designed to instruct employees on both the benefits and risks of Social Media.

Then companies will want to implement networkmonitoring and data loss prevention tools - such as the GV-2010 from Global Velocity to monitor "outbound network" flow of information and automate their security and privacy policies.

We also see that organizations that perform effective training and education programs for employees have better success with information security. In addition, we recommend that companies adopt a position of a "Chief Privacy Officer" to coordinate the privacy and security issues in businesses.

redpoint privacy advisors
www.redpointprivacy.com | 314.222.7979

globalvelocity Next generation cybersecurity solutions
www.globalvelocity.com | 314.588.8555