Managing Online Reputation in a Digital World

September 2013

CSID.COM

CSID®

A part of Experian

TABLE OF CONTENTS

OVERVIEW

Consumers are sharing more information online than ever before, with 27% of time online spent on forums and social networks.[i] In an effort to engage with friends and family and enjoy the benefits of social media, people are also exposing themselves in ways that could lead to unwanted consequences, like reputation damage, identity theft and unemployment. A high price to pay when there are solutions and common sense practices to help manage online reputation.

According to a 2012 Velocity Digital study, 25 percent of Facebook users don't bother with privacy settings. This means anyone can see the content they post which often includes personal identifying information (PII), location, personal details that could be used to reset passwords (pet's name, mother's maiden name), and photos and videos that may tarnish a reputation or provide insight into family, friends and identity that could be used for phishing attempts.

Businesses are not immune. Sixty percent of enterprise businesses worry that employees posting inappropriate or embarrassing content on social media channels can cause brand damage.[ii] Likewise, according to a 2011 Reppler survey, 91% of hiring managers now look at social media when screening job applicants. A 2013 Jobvite survey found that 42% percent of companies have reconsidered job candidates based on the content of their social profiles, including Facebook, Twitter and Google+.

These examples and statistics show that online reputation management is an extremely critical topic for consumers and businesses with many gray areas and uncharted territory.

What types of shared information puts a consumer at risk for data theft? Can we continue to participate openly online while also protecting ourselves? Does an employee's social footprint represent the business he or she works for, and how much control does a business have over this footprint and the content they post?

> ***People are also exposing themselves in ways that could lead to unwated consequences, like reputation damage, identity theft and unemployment.***

With these questions in mind, CSID, a part of Experian, took a look at the topic of online reputation management, including compiling statistics from recent studies on online reputation monitoring and insights from top reputation management experts. This report outlines these results and provides a glimpse into how online reputation can impact people and businesses' reputation and security. This report concludes with an outline of best practices both consumers and businesses can implement to keep their online reputation clean and stay safe online.

INDUSTRY FINDINGS

54% of social media users have been a target of an identity threat
(Javelin, 2011)

69% of enterprise businesses are worried that data leaks via social media can expose the business to risk
(Javelin, 2013)

91% of hiring managers screen job applicants' social media profiles during the hiring process
(Reppler, 2011)

42% of companies have reconsidered job candidates based on the content of their social media profiles
(Jobvite, 2013)

42% of people have scoped someone out on the Internet before doing business with them – and 45% of those have changed their minds about doing business based on something they discovered on the Internet
(MDG Advertising, 2013)

31% of companies have specific policies for employee social media use outside of the workplace
(HCCA and SCCE, 2011)

FROM THE EXPERTS

To shed some light on these statistics and to see exactly how online reputation management impacts consumers and businesses, CSID interviewed two industry experts—Jessica Miller-Merrell, HR consultant and writer of Blogging4jobs and Neil Richards, professor of law at Washington University in St. Louis.

Sixteen minutes of every hour online are spent on social media networks like Facebook, Twitter and Instagram.[iii] Many consumers use these sites to share information with friends and family quickly and easily. They post personal information like full birthdate, addresses, current location, phone numbers, pictures and interests. The problem is that a lot of people don't bother to limit access to this information. According to a Velocity Digital report in 2012, 25% of Facebook users don't bother with any privacy settings, meaning anyone can view the information on their profile, including criminals mining social sites to assist in identity theft, employers vetting social information for hiring decisions, and even sites like Spokeo that aggregate personal information to sell to marketers.

According to Neil Richards, one of the key challenges with online reputation management is the blurring of traditional work life / private life boundaries. When an individual puts something online, they are sharing it with multiple groups that are normally separated in real life. For example, friends and family may be interested in learning about your latest work project on Facebook, but that same information could be used for nefarious purposes in a competitor's hands. It is this blurring of boundaries, and mixing of audiences, that often gets people in trouble online.

Consumers are rewarded for sharing their personal information with free entertainment and relevant content and offers. But at what risk?

RISK #1: IDENTITY THEFT & MISUSE

Social media use and the information an individual shares online puts them at increased risk for identity theft. According to a 2013 Javelin Strategy & Research Identity Fraud Survey Report, 54% of social media users have been the target of an identity threat. The same research reports that accepting a friend request from a stranger can increase the likelihood of being a victim of fraud by 7.4%. Users who "checked in" using GPS have a 7.3% increase in fraud incidence rates. Social media users that uploaded family photos or used an app on a social site saw a 6.5% and 6.4% increase in fraud, respectively.

At CSID, we've also seen online information used for data theft. Cyber criminals will mine information from social media sites and use it to construct a profile of a person that can be used for identity theft or phishing schemes.

Information aggregation sites like Spokeo scan for and collect personal information from sources all over the Internet and create profiles. This information is then sold to marketers for advertising purposes. However, anyone with an internet connection can do a search and find the information these sites collect and access a wealth of personal information name, date of birth, home address, family member names, religion, even salary.

> *One of the key challenges with online reputation management is the blurring of traditional work life / private life boundaries.*

The good news is that you can request for this information to be suppressed and there are services that will monitor for these types of profiles and suppress them on your behalf. Additionally, social media monitoring tools are available and in development to help people concerned about their own online reputations and safety or that of their children and alert them to concerning information.

RISK #2: REPUTATION & EMPLOYMENT

A good online reputation is increasingly important. For a teenager it can mean the difference between getting into a dream college or not. For an adult it could be the key that unlocks a new business opportunity or relationship. The importance of a good online reputation is magnified for job seekers. Most HR departments search for an individual online before making a hiring decision. Per Jessica Miller-Merrell, red flags are raised if an online profile doesn't match the resume or the candidate being interviewed.

Miller-Merrell keeps a running list of employees that were fired because of social media. In 2013, server, Chelsea Welch was fired from Applebee's after posting a customer's receipt on the online website, Reddit. “Bitter Barista,” Matt Watson was fired over his snarky blog. In these instances, it was not just the employee being harmed by the online posting – the business took a hit as well. Miller-Merrell notes that even without a company’s involvement social media technology is being use to craft their online reputation. Companies have to embrace this fact and find a way to educate and train their employees on how to manage their online reputation.

When asked about the legality of using social media information to making hiring and firing decision, Richards says there is still a lot of gray areas when it comes to defining what a person has the right to post online and what an employer has the right to manage and monitor. A Texas school teacher put on Facebook a picture of her holding a Dixie cup, wearing a pirate costume with a sign that said “drunken pirate.” She was fired. In some states this would be legal, in others illegal. It is an ongoing, evolving discussion as companies and legal entities work to define the relationship between employee and employer social media use and what is posted online.

There are a number of legal considerations that should be kept in mind when it comes to online reputation management:

- The National Labor Relations ACT (NLRA) protects online “concerted activity” or the right for employees to communicate online with one another about improving the conditions of their jobs. They cannot be penalized.
- The National Labor Relations ACT does NOT protect employees who post comments online that are “maliciously false,” offensive or inappropriate about their employer or clients. They can be penalized.
- HIPPA compliance mandates that medical information cannot be posted online (including pictures of patients) without permission.
- Regulatory compliance - Pharmaceutical companies engaging in social media must ensure that any conversations about a product, whether they are on Facebook or Twitter, feature the FDA required safety information. Also, any public company needs to be on top of every tweet to monitor whether it complies with the SEC's public disclosure requirements.

RISK #3: BUSINESS CONCERNS

According to Javelin, more than half of enterprise and small businesses are worried about online engagement putting them at increased risk for data theft. This worry is not without cause. Attacks against businesses are becoming increasingly sophisticated. An employee name and email shared on a social network could be used in a phishing attack. Even innocuous information like a high school mascot or a favorite pet’s name could be the answer to security questions asked to reset an employee password and provide access to sensitive business data.

Steve Stasiukonis, a well-known security professional and founder of Secure Network Technologies tested his clients’ network security by creating a fake online identity, then used that identity to join a company’s Facebook page to mine data like email addresses and names. He used this information to send fake phishing emails to employees asking for network login information. The results of his test were astounding – he had an average response rate of 45 to 50 percent with employees volunteering login information and passwords to company networks.[iv] These company credentials could have then been used to access sensitive data like customer credit cards, intellectual property or other login credentials that will provide deeper access into a company’s network.

Some of the businesses that Miller-Merrell advises use a monitoring service that will alert the business if the company name is used in conjunction with certain keywords online. These alerts can be used to monitor what is being said about the company – especially if it is negative – so a business can take corrective action. Keeping a close eye on an employee’s online activities is important. According to Richards, businesses are increasingly liable for the actions employees take online. For example, if Richards hosts a class discussion board on Google+, the University of Washington could be liable for things being said within the discussion.

According to Miller-Merrell, one of the best responses to managing an employee’s online reputation and reducing risk associated with social sharing is to educate and train employees on what types of information they should and shouldn’t share online while preparing for the inevitable misstep that could harm the business.

Morgan Stanley is one of the first financial firms to embrace social media use among its analysts. In 2012, the company rolled out a social media policy that provides a good example of how businesses, even those that are publicly traded and strictly regulated, should approach reputation management. Their policy includes clear rules outlining the types of content an employee can post online, the platforms employees can use to connect with clients and prospects as well as pre-approved content they can share with their networks. The company also monitors usage to ensure no sensitive information is shared and that employees are sticking to the policy. While Morgan Stanley's approach may not work for all businesses and industries, it does ensure that the online reputation of each employee is carefully managed and that the company is minimizing its risk.

To further the discussion on the issues of online reputation management and best practices for consumers and businesses, CSID hosted a webinar as part of their cyberSAFE webinar series titled "Managing an Online Reputation in a Digital World." To view a recording of the webinar, visit http://www.csid.com/resources/webinars/.

RECOMMENDATIONS

MANAGE YOUR PERSONAL ONLINE REPUTATION

- **DO** set and frequently check the privacy settings of your social media profiles, and search for yourself on the Internet to get an idea of your current online reputation.
- **DO** be smart about what you say on the Internet, and what you let others say about you.
- **DO** consider a social media monitoring service.
- **DO NOT** post personal identifying information (PII) on the Internet. This includes birthdate, email address and phone number. This can put you at increased risk for identity theft and put your employer at increased risk for data theft.
- **DO NOT** accept friend requests from strangers or post your location on social media, as this will increase your likelihood of being a victim of fraud.
- **DO NOT** post proprietary information from your employer or customers – past or present.

MANAGE YOUR BUSINESS' ONLINE REPUTATION

- **DO** create a company social media policy that outlines expectations for employees social media activities at the workplace, outside of the workplace and what types of company-specific informaiton that shouldn't be posted online.
- **DO** educate employees and make sure they understand the social media policy and possible consequences of not following it. Teach them why and how their online activities can impact the business and provide them with tools and tips to best manage their online reputations.
- **DO** hire smart from the start and vet potential employee's online reputations from the start. Screen job applicants' online profiles and run Google searches on their names to get a feel for how their online activities may impact your company if hired.
- **DO** consider offering a social media monitoring service to help consumers and employees control social sharing and online reputations
- **DO NOT** ignore what is being said about your company and employees online.

ABOUT CSID

CSID, a part of Experian, is a leading provider of global identity protection and fraud detection technologies for businesses, their employees, and consumers. With CSID's enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection services extend beyond credit monitoring to include a full suite of identity monitoring and fraud detection services; identity theft insurance provided under policies issued to CSID; full-service restoration services; and proactive data breach services.

www.csid.com

ADDITIONAL SOURCES

i Experian, 2013
ii Javelin Research Identity Fraud Survey Report, 2013
iii Experian, 2013
IV Huffington Post, 2013