The Impact of Social Media on Corporate Security: What Every Company Needs to Know

A Cyveillance Report
May 2010

Written by:
Terry Gudaitis, PhD

EXECUTIVE SUMMARY

Social media is an unprecedented phenomenon opening new worlds of opportunity for every organization. While the potential and rewards are seemingly limitless, so are the challenges and risks.

Savvy organizations are making it a priority to re-think outdated 'Internet' policies to include social media, bringing significant changes to their security posture.

Today the lines between an individual's work persona and private persona are permanently blurred. Forums, blogs, and popular social networks like Facebook, LinkedIn and Twitter are just the tip of the social media iceberg. The ubiquitous nature of smartphones and other mobile devices has made the Internet an 'anywhere, anytime' environment in which sensitive company information is often not confined to just behind the corporate perimeter.

While social communities are thriving, so are the scams. Risks such as data leakage pose the biggest threat to most organizations. Social media "squatting" and increasingly sophisticated social engineering schemes are changing the landscape, with consequences ranging from brand reputation damage and lost productivity to potential physical harm to employees.

There are proactive steps every organization can take to strengthen their security posture and minimize potential damage. Addressing these challenges effectively starts with a solid understanding of both the authorized and vast numbers of unauthorized social media users within your organization.

Companies need to have a formal education and training plan in place that meets the needs of all sides of the business. Furthermore, documented social networking policies, ongoing monitoring and a strong organizational feedback structure are essential.

Cyveillance®
a QinetiQ Company

BLURRING THE LINES – THE NEW LANDSCAPE OF COMMUNICATIONS AND SECURITY

With the advent of social media, today's Internet is a far different place from the Web world of even just five years ago. Gone are the days of static content on a Web page that changed slowly, usually measured in days or even weeks. Today, social media has turned the Internet into a thriving, 'always on' environment of constant activity, near real-time postings, chats and tweets, with the latest video uploads to YouTube every minute of the day and night.

The way people engage with the Internet has drastically changed as well. Social media has opened a world of constant 'anywhere, anytime' access thanks to the abundance and popularity of smartphone devices such as the iPhone, BlackBerry®, and Droid. In fact, *Information Week* reported in March 2010 that nearly one in three smartphone users accessed social networks with their mobile browsers, up more than eight percentage points from a year ago.

Furthermore, a new report from the Society for New Communications Research (SNCR) examining the Fortune 500's use of social media in 2009 validated that this is far from a passing trend. While the Fortune 500's use of blogs, online video and podcasts continues to increase, Twitter was the #1 social media channel of choice in 2009. In addition, nearly 20% of the Fortune 500 are podcasting, and 31% are regularly incorporating online video into their blog sites. The adoption of blogs and the explosive growth of Twitter demonstrate the growing role of social media in the business world and its importance as a game-changing customer communications platform.

"Social media isn't a choice anymore – it's a business transformation tool," says Forrester Research's senior analyst Natalie Petouhoff.

Today, that's just half the story. These changes also introduce a multitude of new challenges for both employees and customers.

First, the lines between our 'company selves' and 'personal selves' have all but disappeared. Work comes home, with valuable company data and information of all kinds continually and freely passing from the office cubicle to the dining room table. Personal laptops and phones, for instance, are used as much for work as for checking school soccer schedules, the latest class assignments, or staying in touch with friends.

Second, customers are online recommending brands, sharing experiences with other customers, and praising or criticizing companies they do business with in near real-time. Before social media, customers were barely able to ripple the waters when angry about their dealings with a provider; today they have the tools – and the power - to cause major damage.

Cyveillance®
a QinetiQ Company

Another SNCR study illustrates the vulnerability of brand reputation in the age of social media. Well over half – 59% of respondents – said they use social media to vent anger over their customer service experiences. In addition, 72% of respondents indicated that they sometimes research a provider's customer service reputation online prior to purchasing products or services.

In such an open and thriving new world, it's no wonder scammers, phishers, terrorists, activist groups and criminals of every kind have found a rich, lucrative new 'home,' ideal for everything from money laundering and phishing scams to sending death threats.

While businesses are embracing social media for new growth opportunities, the ones who will be most successful transforming their business over the long run are those who are best prepared.

IDENTIFYING YOUR SOCIAL MEDIA USERS

A key first step in formulating an effective social media policy is to identify your 'authorized' users. Generally these are employees who have approval to speak on behalf of the company using vetted and approved social media platforms – typically professionals in the marketing, public relations and corporate communications departments.

By far, the vast majority of your users fall under the category of 'non-authorized' users -- employees, vendors, agents, partners, lobbyists, and contractors who use social media for both personal and business use, (and have easy access to all kinds of sensitive information) but no authorization to speak on behalf of the organization.

Among the most 'dangerous' of your company's non-authorized users are complete strangers in virtually any public venue. In particular, today's employees routinely travel with a full arsenal of technologies – laptops, smart phones, cameras, video, PDAs, GPS – often forgetting that while in plain sight they're unwittingly 'sharing' confidential information, competitive data, perhaps customer account information through their exposed screens, or simply by "loud talking" their conversations. The person on the plane glancing at your laptop. The waitress overhearing your conversation. The man sharing a bench in the waiting room glancing at your iPhone video, all pose as potential threats to your organization.

These onlookers are then free to post whatever information they find interesting to their own blogs or on sites devoted to eavesdropped chatter such as *http://www.overheardinnewyork.com*.   In every case, social media gives virtually any stranger on the street the power to cause harm to your organization's most precious assets in ways unimagined just a short time ago.

NO IMMUNITY GRANTED: COMMON MYTHS ABOUT SOCIAL MEDIA

"Our company doesn't use social media." "We have a zero tolerance policy toward unauthorized blogging." "We don't allow our employees access to the Internet during work hours."

Following the Breadcrumb Trail to Valuable Competitive Intelligence

John Smith, a busy, high profile executive with a major oil company, routinely travels thousands of miles around the world in the course of his work. As John's plane lands, he uses his iPhone to tell his wife he's arrived safely, even taking a few quick photos to post to Flickr. Unknown to him, through these actions John is also sharing his exact whereabouts via GPS coordinates data in his app, enabling any competitor to easily follow his every move and meeting literally anywhere in the world.

Cyveillance®
a QinetiQ Company

In today's Web world, it just doesn't matter.

The fact is, most of your employees already have handheld devices, gmail accounts, all the common tools of everyday life. All of these tools and devices are outside the control and perimeter of the corporate network. What's more, policies are useless without monitoring and enforcement. While some organizations may claim to have an Internet 'corporate policy' somewhere, it's more often than not buried on a static Web page, its relevance long past expired.

DATA LEAKAGE AND NON-DISCLOSURE

The most common issue organizations face is data leakage and non disclosure violations. Whether through Twitter, chats, blogging, forums, word docs, PDFs or PowerPoint slides, a continual flow of sensitive information, 'inside chatter' and 'dirty laundry' freely enters the Internet for all the world to see.

Make no mistake: Confidential management discussions, disclosure of proprietary trade secret details, who's violating EEOC policies, termination discussions, all manner of confidential and sensitive company information makes its way to social media sites every day.

And in many cases, the release of sensitive information is entirely unintentional. Unwitting corporate employees are posting their corporate email address on eBay and LinkedIn, for instance. But even the most basic company contact information is quickly 'scraped off' and collected by spammers and phishers to be used in their next scheme.

SOCIAL MEDIA SQUATTING

One of the next big trends is 'social media squatting'. Similar to domain name squatting, strangers masquerade as your company, your CEO or simply 'own' your trademark space. Competitors will sometimes use this tactic and purchase every conceivable name related to your company, gaining a powerful – and permanent -- competitive advantage.

The bottomline: you must own your own real estate. With more than 4,000 social media sites active today, it's important to thoroughly examine which ones require your presence to best protect your business. Organizations today need to defensively select and own the right social media space and names. For example, to be properly protected in today's social media world organizations must often go beyond owning their company's trademarked and brand names to actually owning the names of key executives.

A NEW GENERATION OF HACKERS AND PHISHERS, AND SCAMMERS

Social engineering scams are more popular than ever. In a matter of minutes online, a scammer can gather enough specific information about nearly any individual to concoct a very believable email. "Hi, I'm your old classmate from Greenhills High School!" "I see you just sold your house and are moving to my hometown!"

Opening the Door to Discrimination Lawsuits
As people increasingly use blogs and Myspace as personal diaries, naturally that includes frank talk about what happens to them in the course of their work lives. Some law firms and attorneys routinely search for this information, looking for patterns of employee complaints. When they spot a pattern, the next step is often initiation of costly law suits against the company, including class action lawsuits solicited over the Internet.

Getting Personal: The High Cost of Calling in 'Sick'
An individual posing as a high profile executive for a major company sent tweets indicating he was quite ill. As the false news spread, stock prices dove, sending a wave of financial panic. After 24 hours of chaos, the 'real' executive got online with assurances he was fine, but not before the false news shook the company, taking a big toll on the balance sheet … or allowing someone to make a handsome profit by short-selling.

Cyveillance®
a QinetiQ Company

Even a seemingly innocent tweet can lead an unsuspecting user right into a landing page with destructive malware.

Hackers, phishers and scammers of every variety are using social media networks as ideal gateways to bypass corporate security measures. And it's working.

Likewise, phishing activities have leveraged social media to launch even more lucrative 'whale phishing' schemes that target individual, well off, high profile executives with high net worth bringing bigger payoffs.

THE HIGH COST OF INACTION

Companies who adopt a 'wait and see' approach can find themselves in the unenviable position of incurring financial losses and more.

Harm to brand reputation. Damage to a company's brand reputation is often irreparable, and in today's world requires more than just sitting back. In some cases, companies are proactively contacting those who launch complaints, immediately initiating a dialog to understand the issue, and effectively using the very same communications platform as the complaintant.

Lost productivity. Employees using Twitter, posting photos during business hours, participating in chats and the like take a heavy toll on overall productivity, costs that add up exponentially over time. However, even more time may be wasted if social networks are blocked completely from employees. When blocked, employees will often simply resort to their smart phones, MiFi's, walking to the parking lot, the car, or to the local coffee shop next to the office to engage in social networking. They will also often become very vocal about the fact that their place of work is blocking access.

Strains on bandwidth. Make no mistake, your employees know where the free wi-fi zones are in your building and aren't shy about making use of them. This misuse eats away at precious company bandwidth and can quickly add up to significant costs.

TAKING ACTION: IMPLEMENTING EFFECTIVE CORPORATE SOCIAL MEDIA PRACTICES

While the challenge may sound daunting, there are steps every organization can take to ensure a stronger security posture.

First, proper education and training are imperative. Every employee should be well apprised of the vulnerabilities of using social media within the company and at home, personally. The fact is, most employees simply don't fully understand the level of risk and the potential devastating consequences when it comes to social media. A standard "Cybersafety 101" Class, for instance, is a good place to start. In addition, more specialized training is a good idea for high profile executives who are often victims of choice for savvy fraudsters.

LinkedIn leveraged for Social Engineering
A scammer sets up a profile on LinkedIn for a company executive and proceeds to build out his/her network by targeting actual company employees. Using LinkedIn's user to user email functionality the scammer can direct unsuspecting users to rogue sites that distribute malware payloads or leverage his new-found relationships to uncover proprietary information.

Activists Move at the Speed of Twitter
At high profile public events, activists intent on disrupting activities are communicating with each other in real time. Using Twitter, they share precise information on the whereabouts of police, the exact location of high profile individuals, etc. Demonstrators can then change locations on the fly, even upload pictures. For the organization targeted in the event, monitoring Twitter can provide valuable lead time for security teams, and a greater ability to protect themselves and their people.

Cyveillance®
a QinetiQ Company

Second, solid Social Networking Policies must be put in place, monitored and enforced. It's a good idea to have two sets of policies, one for authorized users who have a legitimate level of need and another for unauthorized users. When creating policies, there are a multitude of variables to consider. How strict or how liberal should your policies be? Should employees be allowed to talk about sensitive topics such as salary? The name of their supervisor? Projects they're working on? It cannot be overemphasized that fully monitored and enforced policies must be established that everybody understands.

Third, proactive, ongoing monitoring is essential for success. Every organization must take responsibility for knowing what the latest and greatest 'thing' is, beyond Twitter. It's also important to let employees know that you're not just 'closing the gates'; it's for everyone's protection.

Finally, departments must commit to coming together to create a rock solid organizational feedback loop. It's all too common to point the finger at another department, but the fact is: When there's an incident, it's more than a PR issue. It's more than likely a security, human resources, legal, IT and maybe even a physical security issue. Nearly every department has a role to play that can make or break an organization's social media policy.

CONCLUSION

In the 'wild west' of social media, organizations must take responsibility for developing a proactive strategy that protects all sides of the business.

Companies must start with a good understanding of their social media uses and users within their organization, developing relevant, enforceable policies that recognize the blurred lines between employees' work and personal online lives.

Ultimately, businesses that will be most successful in leveraging social media are those with a full understanding of the risks as well as the rewards, and are prepared with the most effective methods for monitoring and policy enforcement.

Going Viral: The Superpowers of a Single Disgruntled Customer
Jane Doe is a very unhappy customer of Company ABC. Jane starts a blog, detailing her dissatisfaction with the company. She also posts the content to a few forums, getting angrier by the hour. In fact, she starts Ihateproductx.com, continuing to blog away. Jane asks other like-minded individuals to register more, using the same product name. Within hours, a fringe element fans the fire. In fact, they escalate the situation to the point of sending death threats. A single brand issue has changed to a life or death situation within 72 hours.

Cyveillance®
a QinetiQ Company

ABOUT THE AUTHOR

Dr. Terry Gudaitis is Cyber Intelligence Director at Cyveillance and a leading authority on cyber security and cyber crime profiling and psychology. She is focused on the human psychology and security aspects of malicious Internet threats, leading the Cyveillance team of cyber intelligence analysts.

Since 1987 she has provided consultation and leadership in cyber crime to public and private industry including SAIC (Science Applications International Corporation) and NSEC (Network Security Corp.), federal intelligence agencies and bureaus, and law enforcement, focusing on domestic and international security issues.

Dr. Gudaitis has served on the United States Secret Service Advisory Board for Insider Threat and trained investigators at the National Center for Missing and Exploited Children.
Dr. Gudaitis holds an M.A. in Behavioral Science and a Ph.D. in Criminology from the University of Florida. She is a frequent contributor to numerous security-related journals and a regular speaker and presenter at national cyber security events.

ABOUT CYVEILLANCE

Cyveillance, a world leader in cyber intelligence, provides an intelligence-led approach to security. Through continuous, comprehensive Internet monitoring and sophisticated intelligence analysis, Cyveillance proactively identifies and eliminates threats to information, infrastructure, individuals and their interactions, enabling its customers to preserve their reputation, revenues, and customer trust. Cyveillance serves the Global 2000 and OEM Data Partners – protecting the majority of the Fortune 50, regional financial institutions nationwide, and more than 30 million global consumers through its partnerships with security and service providers that include AOL and Microsoft. Cyveillance is a QinetiQ Company. For more information, please visit www.cyveillance.com or www.qinetiq-na.com.

Cyveillance®
a QinetiQ Company