The Impact of Social Media On Information Security
What Every Company Needs To Know

A CYVEILLANCE WHITE PAPER | MAY 2015
# Table of Contents

Executive Summary ................................................................. 3  
Blurred Lines: The New Landscape Of Communications And Security ...... 4  
Identifying Your Social Media Users ............................................. 7  
No Immunity Granted: Common Myths About Social Media ................. 9  
Data Leakage And Non-Disclosure Violations .................................. 10  
Social Media Squatting ............................................................... 11  
A New Generation Of Hackers, Phishers, And Scammers ....................... 12  
The High Cost Of Inaction ............................................................ 13  
Taking Action: Implementing Effective Corporate Social Media Practices. . 15  
Summary ................................................................................. 16
Executive Summary

Social media is an unprecedented phenomenon that has opened new worlds of opportunity for organizations around the globe. 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Savvy organizations are making it a priority to re-think outdated ‘Internet’ policies to include social media, bringing significant changes to their security posture.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 increasingly 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 ‘anywhere, anytime’ Internet a reality, and sensitive company information is no longer confined to the limits of the corporate perimeter.

Social platforms are thriving, but so are schemes to use them for crime and ill will. Risks such as data leakage pose the biggest threat to most organizations. Social media ‘squatting’ and sophisticated social engineering schemes are changing the landscape for security professionals, with consequences ranging from brand reputation damage and lost productivity to potential physical harm to employees and executives.

There are proactive steps every organization can take to strengthen their security posture and minimize potential damage. Addressing these challenges effectively begins with a solid understanding of both the authorized and 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, a strong organizational feedback, ongoing monitoring, and structure documented social networking policies are essential.
With social media now a part of daily life for millions of people around the world, the Internet is a far different place from the online world of even a few years ago. Gone are the days of static content on a website that changed slowly. Today, social media has turned the Internet into a thriving, ‘always on’ environment of constant activity, near real-time postings, chats, tweets, and millions of video uploads to YouTube, Vine, and other popular platforms every minute.

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 Android. In fact, statistics from Pew Internet Project’s research for mobile technology show that as of January 2014, 90% of American adults owned a cell phone and, 42% of American adults own a tablet computer.¹ There are more connected mobile devices on earth than the number of people. “No other technology has impacted us like the mobile phone. It's the fastest growing man-made phenomenon ever – from zero to 7.2 billion in three decades,” said Kevin Kimberlin, Chairman of Spencer Trask & Co.² The majority of digital media is consumed with mobile applications, surpassing even desktop usage.³ In terms of social media, personal use of social networking applications accounted for an estimated 46% of all smartphone activity and 19% of all tablet traffic.⁴

---
⁴ [http://mobilemarketingmagazine.com/content/social-networking-makes-nearly-half-smartphone-traffic](http://mobilemarketingmagazine.com/content/social-networking-makes-nearly-half-smartphone-traffic)
Furthermore, data from the Center for Marketing Research at the University of Massachusetts Dartmouth that focused on the Fortune 500’s use of social media validated that this is far from a passing trend. Their research suggests that companies are now relying almost exclusively on social media to reach consumers and that only 144 of Fortune 500 companies (23 percent) currently have public-facing corporate blogs. Sixty-two percent of Fortune 500 companies currently have an active Twitter account, while fifty-eight percent currently have a Facebook page. The explosive growth of Twitter and Facebook accounts for Fortune 500 companies demonstrates the growing role of social media in the business world and its importance as a game-changing customer communications platform.5

This rapid, ongoing growth has introduced a multitude of new challenges for both employees and customers. The lines between our ‘company selves’ and ‘personal selves’ have all but disappeared. Work comes home or goes to the coffee shop, with valuable company data and information of all kinds continually and freely passing from the office cubicle to the dining room table to the counter at the local café. Personal laptops and phones are used as much for work as for checking soccer schedules, the latest class assignments, shopping, and staying in touch with friends. Customers are online recommending brands, sharing experiences...

---

Social Media Apps:
New Security, Compliance Risks

One of the most challenging aspects of social media is that it is constantly evolving. Privacy and security concerns are often overlooked in the race to roll out new features and integrate platforms into the lives of even more users. For example, LinkedIn introduced a mobile app in late 2013 called “Intro” that inserts LinkedIn profile information into the emails of Apple iOS users. The app is ostensibly designed to provide users an extended introduction to whoever is sending them messages by automatically showing their LinkedIn profile. Once it is downloaded, all sent and received emails are redirected to LinkedIn proxy servers. With this process, LinkedIn decrypts the sent email to include the profile information, and then reencrypts it. Many security researchers have likened this to a “man-in-the-middle attack,” in which hackers intercept Internet traffic en route for malicious purposes. An additional security concern is that the app may violate many employers’ security and compliance policies, as employees using the app would technically be disclosing sensitive and classified data to a third party.

---

5 http://www.umassd.edu/cmr/socialmediaresearch/2013fortune500/
Creating a Social Media Policy: Why One-Size-Fits-All May Not Work

When creating social media policies, there are a multitude of variables to consider. How strict or how liberal should your policy be? Should employees be allowed to talk about sensitive topics such as their salary or the name of their supervisor? Projects they’re working on? What about employees “checking in” at headquarters or client locations using location-based social networking websites like Foursquare? What about photos and videos posted to YouTube, Vine or Instagram from sensitive locations like security operations centers? How do you deal with global employees who are using social media platforms like Weibo and Badoo for example, or who may have different cultural expectations around privacy even when posting to public platforms? What about employees who use social media as part of their daily job, such as in marketing and public relations? The need to establish and enforce policies that take into account a broad range of platforms and users cannot be overemphasized.

with other customers, and praising or criticizing companies they do business with in real-time. Consumers share their purchases socially on social media sites, and 70 percent of Millennials say that they are more likely to make a purchase based on their friends’ social media posts. 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.

A study revealed that 42 percent of consumers who use social media for customer service issues expect a response from the business in an hour. Responding is important because 46 percent of web users look towards social media when making a purchase.

In such an open and thriving environment, 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 to deal with both the risks and benefits it presents.

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, smartphones, 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 talking without thinking about who might be overhearing their conversation. The person on the plane glancing at your laptop screen. The waitress eavesdropping on your conversation. The man sharing a bench in the doctor’s office waiting room glancing at your iPhone. All pose potential threats to your organization.
These onlookers are free to post whatever information they find interesting to their blogs or on websites 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.

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. While GPS tagging can easily be disabled on most apps and devices, many users don’t take this easy but often over-looked step.
“Our company doesn’t use social media.”

“We have a zero tolerance policy toward unauthorized blogging.”

“We don’t allow our employees to have access to the Internet during work hours.”

In today’s online 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, more often than not, it’s buried on a static web page, its relevance long past expired.
The most common issues organizations face are 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, which companies are violating EEOC policies, termination discussions, and all manner of confidential and sensitive company information makes its way to social media sites every day.

In many cases, the release of sensitive information is entirely unintentional. Corporate employees often use their corporate email address for their contact information on eBay and LinkedIn, for instance. But even the most basic contact information can quickly be ‘scraped’ and collected by spammers and phishers to be used in their next scheme.

Opening the Door to Discrimination Lawsuits

As people increasingly use blogs and Facebook as personal diaries, naturally that includes frank talk about what happens to them in the course of their work lives. 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.
An ongoing trend impacting brands is ‘social media squatting’. Similar to domain name typosquatting or cybersquatting, strangers masquerade as your company, your CEO, or simply ‘own’ your trademark space in social media platforms. Competitors may even use this tactic and register every conceivable name and social media page that could be related to your company, gaining a powerful – and sometimes permanent – competitive advantage.

The bottom line: you must own your 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 protect their social media space in addition to their domain names. To be properly protected in today’s social media world, organizations must often go beyond protecting their company’s trademarked and brand names to protecting the names of key executives, too.

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 to reassure everyone that 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.
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!” or “I see you just sold your house and are moving to my hometown!”

Even a seemingly innocent tweet can lead an unsuspecting user right to 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 high-profile executives.
Organizations that adopt a ‘wait and see’ approach can find themselves in the unenviable position of incurring financial losses and long-term damage to their brand.

Harm to Brand Reputation
Damage to a company’s reputation is often irreparable, and in today’s world, brands can’t afford to sit on the sidelines and ignore customer complaints. 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 complainant.

Lost Productivity
Employees using Twitter, posting photos to Instagram and Facebook during business hours, participating in chats and the like take a heavy toll on overall productivity – costs that can add up exponentially over
Activists and Hacktivists: Moving at the Speed of Twitter

At high-profile public events, activists and hacktivists intent on disrupting activities communicate with each other in real time. Using Twitter, they can share precise information on the whereabouts of police, the exact location of high-profile individuals, and other details. Demonstrators can then change locations on the fly, even uploading photos. For organizations targeted in events like this, monitoring Twitter can provide valuable lead time for security teams, and a greater ability to protect themselves and their people.

Strains on Bandwidth

Make no mistake, in addition to the toll that heavy social media usage can take on your network, your employees know where the free Wi-Fi zones are in your building and aren’t shy about making use of them to access content on their mobile devices. This misuse eats away at precious company bandwidth and can quickly add up to significant costs.

Data Leaks and Disclosures

Without enforceable policies and ongoing monitoring, it’s easy for employees to turn into your biggest “accidental threat” by leaking data that they shouldn’t. Information that makes its way onto and via social media generally falls into four broad areas: intellectual property, customer data, operational data, and infrastructure data. Intellectual property may include documents, presentations, product specifications, and proprietary code. Customer data can include personal and health information, credit card numbers, and login credentials. Operational data and infrastructure data can be harder to identity and monitor, but can include rumors of mergers and acquisitions, discussion of production stoppages or delays, launch dates, leadership transitions, technical discussions, and other chatter.

Information that leaks out onto and via social media falls into four broad areas:

- Intellectual Property
- Customer Data
- Operational Data
- Infrastructure Information
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 and related platforms, such as file sharing sites, within the company and at home. 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 “Cyber Safety 101” class is a good place to start. In addition, more specialized training should be provided for high-profile executives who are often the victims of choice for savvy fraudsters.

Second, solid social networking policies must be put in place, monitored and enforced. You may wish to develop two sets of policies: one for users who are authorized to officially post to social media on behalf of the organization, and another for employees who are not.

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’ and that social media guidelines and policies are designed 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 public relations 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.

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. She even registers a domain name, ihateproductx.com, where she hosts her blog. While she’s at it, she also posts updates to Twitter every 15 minutes to vent her frustrations and direct people to her blog. Jane asks other like-minded individuals to register similar domain names, 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.
As social media continues to grow and become a part of daily life for millions of people, organizations must take responsibility for developing a proactive strategy that protects all facets of the business while taking advantage of the opportunities it offers to engage with customers, increase brand awareness, and generate revenue.

Organizations must start with a good understanding of their current online and social media profile, and where they may be at risk from not having an official presence. They must also consider how their employees and executives are using social media, developing relevant, enforceable policies that recognize the blurred lines between work and personal online lives. Employees may have different objectives and needs for using social media in their respective work roles, and banning access to social media entirely may backfire.

Ultimately, the 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 those that are equipped with the most effective methods for monitoring and policy enforcement.
While your network may be secure, do you have visibility beyond the perimeter? Security is no longer about what you can see. What you can’t see is where the true threats hide.

Cyveillance offers an easy-to-use platform that enables security professionals the ability to see beyond the perimeter. Our solutions identify cyber and physical threats and risks across the globe, allowing you to mitigate and eliminate them before they disrupt your business.

We go beyond data to provide the threat intelligence that you need to achieve your organization’s business goals. Contact us today to learn more and get a free trial.

www.cyveillance.com/cyberthreatcenter
Cyveillance is the leading provider of cyber threat intelligence, enabling organizations to protect their information, infrastructure, and employees from physical and online threats found outside the network perimeter. Founded in 1997, Cyveillance delivers an intelligence-led approach to security through continuous, comprehensive monitoring of millions of online data sources, along with sophisticated technical and human analysis. The Cyveillance Cyber Threat Center, a cloud-based platform, combines web search, social media monitoring, underground channel information, and global intelligence with investigative tools and databases of threat actors, domain names and IP data, phishing activity, and malware. Cyveillance serves the Global 2000 and the majority of the Fortune 50 – as well as global leaders in finance, technology, and energy – along with data partners and resellers. For more information, visit www.cyveillance.com.

Cyveillance is a wholly-owned subsidiary of QinetiQ, a FTSE250 company which uses its domain knowledge to provide technical support and know-how to customers in the global aerospace, defense and security markets. For more information, visit www.qinetiq.com.