



The Power to Prevent:
It's the Next Generation

FIDELIS SECURITY SYSTEMS, INC. 4416 EAST WEST HIGHWAY, SUITE 310, BETHESDA, MD 20814



How Government Agencies Can Leverage the Power of Social Networking While Mitigating Risk

Fidelis Security Systems
David Etue, VP, Product and Markets
February 2010

Table of Contents

Value of Social Networking to Government Agencies.....	3
Risks of Social Networking	4
Unlocking the Value by Mitigating the Risks	6
The Fidelis Extrusion Prevention System®: Visibility and Control for Social Networking.....	7

Value of Social Networking to Government Agencies

Social networking is quickly becoming part of the fabric of how we communicate and collaborate. With value from micro-level personal networking to macro-level citizen outreach, social networking has already illustrated significant potential in government agencies, private enterprises, and our personal lives. Apps.gov defines social networks as "a set of internet tools that enable shared community experiences." This shared experience is the power that has driven social networking and transformed the user experience from informational to collaborative. Whether public, limited, or private social media site, anyone with access is now a publisher, enabling faster information sharing and quicker feedback cycles across a much broader audience. These new social platforms have provided new approaches to many critical enterprise functions including identifying, communication with and gathering feedback from constituents (e.g., Facebook, Ning); locating expertise (e.g., LinkedIn); providing new communication platforms (e.g., twitter); and collaborating with a community, small or large (e.g., wikis).

It's clear that government organizations see value in these platforms for enabling "open government," making it easier to communicate government information, deliver services or entitlements, and engage constituents in the policy-making process. For example:

- GSA has created a Social Networks section in [Apps.gov](#), with custom terms of service for Federal agencies with sites including Facebook, LinkedIn and MySpace.
 - As of December 2009 over 27 Federal government agencies have signed terms of service agreements with Facebook.

Social Networks

Social Networks are a set of internet tools that enable shared community experiences. A community, in this context, is a group of people with common interests who connect with one another to learn, work, organize and socialize. Social media tools make it easier to create and distribute content and discuss the things we care about. Social media includes various online technology tools that enable people to communicate easily via the internet to share information and resources. Social media can include text, audio, video, images, podcasts, and other multimedia communications.

 <p>FriendFeed Price: Free</p> <p>FriendFeed is a real-time feed aggregator that consolidates the updates from social</p> <p>ENROLL ></p>	 <p>FaceBook Price: Free</p> <p>Facebook is a free-access social networking website mission that gives people the power to</p> <p>ENROLL ></p>	 <p>MySpace Price: Free</p> <p>MySpace is a social networking website with an interactive, user-submitted network of friends,</p> <p>ENROLL ></p>	 <p>LinkedIn Price: Free</p> <p>LinkedIn is an interconnected network of experienced professionals from around the world,</p> <p>ENROLL ></p>
---	--	---	---

- [DHS has implemented OurBorder on Ning.](#)
- Many state and local governments have established a social networking presence. Examples include [Arlington County, Virginia on Facebook](#) and [Montgomery County, Maryland on Twitter.](#)
- Fort Belvoir recently used [Facebook](#) and [twitter](#) to facilitate communications during a snow emergency (source: <http://www.armedandcurious.com/2010/01/shooting-and-blizzard-show-power-of.html>)
- The US Forces in Afghanistan are using social media to [NPR: U.S. Military In Afghanistan Turns To Twitter, Facebook & YouTube](#)

Despite all of this interest, however, most organizations are still blocking all access to social networking, or just allowing access from a small number of public affairs personnel due to the risks of inappropriate use and leakage of agency sensitive information.

Risks of Social Networking

Social networking unfortunately also comes with risks, which can be reputational, security, or compliance related. These risks are causing many organizations to continue blocking social networking access from their networks, thereby preventing these risks, but also social networking's benefits, from becoming a reality.

The social networking threat landscape can be summarized into the following areas:

1. Unapproved Users Speaking on the Agency's Behalf

As social networking provides all users the opportunity to post and collaborate, many organizations are concerned that user posts will be considered official agency communications. Even when a user is able to speak on behalf of an agency, authorized comments may be limited to a particular topic. This risk exists in many other mediums today, but is more salient with social networking because the communications are written, more users are using social networking compared to other alternatives (press interaction, bulletin boards, etc.), and publication/republishing of comments is instantaneous, broad, and for the most part unmoderated.

It is important to note that nothing prevents individuals from participating on social networks. Even if access to social networking sites is blocked in the workplace, most users have alternative internet access including home internet connections, mobile devices, and public access locations.

2. Inappropriate Posting of Agency Sensitive Information

Perhaps one of the most significant risks of social networking is the unauthorized disclosure of agency-sensitive information. Leakage or loss of control of protected or sensitive information, whether about individuals (employees, citizens) or digital assets ranging from national security information to security plans to legally protected information, could have serious national security and compliance implications, both of which can lead to significant erosion of constituent trust.

"Social networking applications are increasingly being used in a business context, or accessed by employees using corporate computing resources, raising new concerns that these sites present a potential risk for data leakage," said Trent Henry, Principal Analyst, Burton Group. "Like e-mail, webmail, and instant messaging, social networking applications are a potential avenue for sensitive data leakage."

3. Malicious Code Distribution

Social networking sites have been used to distribute malware. Due to the breadth and speed of distribution that social media sites can provide cybercriminals, this trend is likely to accelerate. The "Koobface" virus in late 2008 is the best known example of malware that used social

networking for distribution. When infected, the virus posts links to other Facebook users' pages with comments to entice the user to click on the link, like "*Are you sure this is your first acting experience?*" When users click on the link, they are presented with malicious code to further propagate the virus as well as conduct other potentially harmful activities.

4. Social Engineering to Exfiltration of Agency Sensitive Information

Social engineering, as defined by the infamous hacker and social engineer Kevin Mitnick, is the act of using "influence and persuasion to deceive people by convincing them that the social engineer is someone he isn't, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology." Social networks are an attractive platform for these activities, as they provide a mechanism to create trust to extract information.

This trust is typically accomplished via one of three mechanisms:

1. Fake social network accounts purporting to be someone they are not;
2. Compromised account of a user already trusted in the site;
3. Social networking applications within the site.

In the first scenario, a user creates an account on a social networking site. In their profile, they list that they work at a large government contractor working at a particular agency, and previously used to be a federal employee at a different agency. They send networking requests to others who may want to network with someone with their profile. Once established, they then may ask questions of another agency to attempt to extract information that shouldn't be shared. Since it appears this person is working on the government's behalf, many users will share information with them.

In the second scenario, a Facebook account is targeted for attack. The hacker gains credentials to the account (often via a dictionary or spear-phishing, a targeted form of phishing). Once they have access to the account, they will login and send their requests as if they were the user. I recently experienced this when one of my friend's Facebook account was compromised. The threat actor sent me an instant message from a friend's account in Facebook informing me that he was traveling to a foreign country, was robbed, and needed me to quickly send him money via Western Union as he desperately needed cash to be able to get back to the United States. Assuming this was a hoax, I called my friend on his cell phone to find him at work in the U.S. and then reported the incident to Facebook security and Western Union's fraud department. This instance was personal and financial, but a similar attack could easily be used to extract agency sensitive information.

The final scenario takes advantage of the applications that are able to be deployed by third parties on social networking sites. Facebook has been the clear leader in allowing third parties to develop applications to date, but the "app economy" is growing quickly. In this scenario, the threat actor writes a third party application (often a quiz) designed to extract information from the targets. For example, a quiz could be developed for "How Great of an XYZ Agency Employee are you?" The quiz would ask questions like "how long have you been a federal employee", "what office you work in", "what contractors you do business with", "how much spending you oversee", etc. When the user is done and submits the quiz, they get a score of "Fabulous

Employee" and the threat actor gets a list of information that alone may be useful or can be used to extract other information.

Unlocking the Value by Mitigating the Risks

The risks presented in social networking are real, but fortunately so are the benefits. An organization doesn't have to say "No" and block access to social networking sites, but instead can enable the business use of social networking while mitigating the risks.

Many of the risks of social networking can be mitigated with the following recommendations:

- 1) Ensure existing employee codes of conduct policies cover social networking. There may be one policy governing all activities, or multiple policies, but it is important this is not just a computer use policy. The computer use policy should cover whether it is acceptable to use social networking only for work or for work and personal activities. However, it is important the policy also cover what activities the employee (or contractor) can do on behalf of the agency. If it is deemed the policies require updating to cover scenarios related to social networking, it is important to communicate and train the users on the updated policy. This will help address the risk of an unapproved employees speaking on the agency's behalf. It will also provide a mechanism for actions against any employees that violate these policies.
- 2) End user training on benefits, risks, policies, and agency goals on the use of social networking. It is important to communicate to employees and contractors what the agency is looking to accomplish using social networking and their role in it. Much like you would brief an executive to prepare for a press briefing or Congressional testimony, this is the opportunity to prepare the user as to how they can support the agency's mission using social networking, and to explain appropriate versus inappropriate use. This should explain the goals of social networking, who has the authority to speak on an agencies behalf, what actions and activities are appropriate, and who to contact with questions and issues.
- 3) Create official profiles for the agency, sub-agency, and key executives on the major social networking sites, particularly any site approved in apps.gov, to avoid creation of fake accounts used for impersonation. This should be done even if they will not be used, and can be marked as such.
- 4) Ensure anti-virus solutions at the endpoint and gateway are inspecting communications to and from social networking sites, and that updates are applied in a timely manner. This should be a standard feature of the majority of enterprise-class anti-virus solutions, and already implemented at the majority of Federal agencies.
- 5) Implement technical controls controlling how social networking can be used and what content can be posted. Unfortunately most technologies claiming to help mitigate the risk of social networking can only turn a particular site on or off--forcing an organization to have to accept all of the technical risks associated with social networking to garner the benefits, or get none of the benefits by blocking the sites completely. Some of these tools may be able to allow social networking for a particular user population in the network, but unfortunately they still allow any content to be posted.

In order to be able to allow the agency to gain the value of social networking while mitigating the risk of inappropriate posting of agency sensitive information or exfiltration via social engineering, a technical solution that understands the context of each social networking communication transaction is required. At a minimum, the technical solution needs to be able to identify:

1. The user or system posting the information;
2. What type of information is being posted;
3. What social networking site the information is being posted to;
4. What type of transaction in the site (e.g., post, instant message/chat, third party applications, e-mail/message).

Beyond identifying these attributes, the solution also needs to be able to understand the context between them. Examples include:

- Public Affairs is allowed to post agency updates, but no other users;
- No agency sensitive information can be posted to any public social networking site;
- No information can be posted to third party applications;
- Only certain employees can converse (via posts or chat) with citizens or constituents.

Finally, the solution needs to be able to prevent an unauthorized communication. If the solution only can detect a violation, but not prevent it from occurring, incidents still can occur, so the ability to remediate a post that violates policy is critical.

The Fidelis Extrusion Prevention System®: Visibility and Control for Social Networking

Fidelis Security Systems, the leader in next-generation network security solutions, is the only solution to provide the visibility and controls necessary to understand both the content and context of information posted to social network applications, thus enabling the use of social networking for business purposes while preventing leaks of sensitive information, digital assets, and identity information. Unlike other solutions that use simple site or user level blacklisting, the company's flagship solution, Fidelis XPS™, features granular policy controls for traffic to social networking sites as well as specific controls for post, chat, and mail functions for leading social networking applications. With support for Facebook, LinkedIn, MySpace, Plaxo, Twitter, Orkut, Friendster, Hi5, Ning, and Badoo, Fidelis XPS allows legitimate business to flow freely through approved channels, including social networks, while potentially risky behaviors are detected and remediated.

For social networking, and your broader network traffic, Fidelis XPS provides visibility of and control over the applications running on the network, enabling your organization to see how the network is used for communication. With port and protocol independence and proxy-less inspection native to its Deep Session Inspection™ platform, Fidelis XPS goes beyond packet analysis by providing deep session inspection and payload reassembly, giving organizations the



ability to manage applications, content, and the context between them, all without the hassles of desktop and server configuration changes, and without negative impact on performance. With Fidelis XPS' Deep Session Inspection platform, and its native port-independent inspection covering all 65,535 ports, it provides the most robust architecture for visibility and control of the applications and content in use on the network.

Fidelis XPS provides the only network security solution with specific features to manage the use of social networking applications, enabling organizations to use social networking sites for business gains while managing the risk of data leakage and data exfiltration. Unlike web filtering technology that can only turn a site or its components on/off, or DLP solutions that can inspect content but lack the context required to understand the actions/modes in a social networking site, Fidelis XPS provides the only solution to understand the different modes in a social networking application (e.g. facebook has Post, Chat, Mail, and Application), content analysis and the context between them. Social networking has become ubiquitous in today's enterprises, often with customers demanding participation from their suppliers. As social networking has become common place for business, it is typically no longer practical to blacklist the entire site, but the risks of data leakage remain high with many surveys showing social networking only behind e-mail, web mail, and instant messaging (IM) for the likelihood of data leakage. Fidelis XPS provides comprehensive visibility into and control over social networking network traffic, and enables fine grained controls of particular social networking activities to allow an organization to extract business value from social networking while mitigating the risk of data leakage.

FIDELIS SECURITY SYSTEMS, FIDELIS EXTRUSION PREVENTION SYSTEM, FIDELIS XPS, the FIDELIS SECURITY SYSTEMS logo, and/or other FIDELIS SECURITY SYSTEMS products referenced herein are trademarks of Fidelis Security Systems, Inc. Copying, use or distribution of any material contained herein is expressly prohibited. *Copyright © 2009 Fidelis Security Systems, Inc. All rights reserved.*