BRITISH COLUMBIA | Office of the Chief Information Officer

An Information Security Perspective on the Safe Use of Social Media:

Suggestions from the CISO on Balancing Risks and Opportunities

Information Security Branch

Created October, 2010
Updated January, 2014

This document was prepared by the Chief Information Security Officer (CISO) for the Province of British Columbia. It serves as a companion to the publication *Guidelines for Conducting Public Engagement, Specific to Social Media* and provides an information security perspective on the use of social media.

The ***Guidelines for Conducting Public Engagement, Specific to Social Media*** document describes:

- the B.C. Public Service philosophy on using commercial social media,
- key considerations when using social media,
- the protection of privacy and the concepts of personal information collection and disclosure,
- intellectual property and records management when using social media, and
- the principles of Being Professional, Being Personable and Being Relevant when using social media.

The document can be found at http://www.gov.bc.ca/citz/citizens_engagement/index.html

The intention of ***An Information Security Perspective on the Safe Use of Social Media: Suggestions from the CISO on Balancing Risks and Opportunities*** is:

- to help understand the information security risks to consider in deciding to adopt social media, and how to mitigate these risks,
- to create an awareness of the most common security threats when using social media, and
- to provide some considerations and guidance for employees.

Gary Perkins
Chief Information Security Officer & Executive Director
Information Security Branch, Office of the Chief Information Officer
Ministry of Technology, Innovation and Citizens' Services
Province of British Columbia
http://www.gov.bc.ca/informationsecurity

Social Media in the B.C. Public Service: A Service and Risk-Based Decision

Program managers and administrators throughout the British Columbia government are giving thought to the ways in which they can maximize opportunities by adopting social media tools as a beneficial part of their operations. Whether the purpose is to take advantage of a more collaborative approach to conducting business, to engage the public, or to incorporate the ever increasing wave of social media technologies into the workplace, there are both risks and opportunities to be considered and weighed in making these decisions.

Social media tools (such as wikis, blogs, personalized homepages and social network sites such as Facebook, Twitter and LinkedIn) were developed for consumers but their popularity and widespread use have resulted in organizations assessing the potential of these tools for interacting with the public. Bringing these tools into the B.C. public service has become a natural technology evolution.

If you have questions or concerns regarding your information security requirements, contact your Ministry Information Security Officer who can assist you with assessing risks and selecting appropriate security controls. They can also work with you to determine if a Security Threat and Risk Assessment is appropriate for your initiative.

The decision to adopt social media tools and services is a business decision, not a technology decision. If you want to use Social media in your program, the first place to start is the *Guidelines for Conducting Public Engagement, Specific to Social Media* published by the Workforce Planning and Leadership Branch, Ministry of Citizens' Services at http://www.gov.bc.ca/citz/citizens_engagement/index.html.

Social media tools do not focus on a specific technology but on a new way of using the Internet. Many of the social media security threats, therefore, are not necessarily specific to an application, but are instilled in the many new ways that the technology is used. The purpose of this document is to create an awareness of some of the information security risks and threats in adopting and using various forms of social media and to provide some recommendations on mitigating these risks.

What are the Risks to Consider with Social Media?

All information technology (including servers, routers, desktops, laptops and mobile devices) are the targets of highly-organized, financially motivated criminals who use their IT knowledge and skills to launch persistent, pervasive and aggressive attacks against governments, corporations, critical infrastructures, institutions in every sector (education, health, justice). While there are other reasons for launching cyber-attacks, such as political disruption, espionage, or malice, in most cases the primary motivator is to acquire personal financial information that has economic value in the underground economy.

Cyber-attacks on B.C. government IT systems are attempted every day. The government has numerous security and risk management tools in place, along with the human resources needed to manage and monitor the IT infrastructure. Studies conducted by security professionals on organizational security breaches across the world have consistently shown that **most successful breaches are the result of human behaviour – sometimes due to malicious intent of employees, but primarily due to lack of knowledge, or the failure of users to adhere to safe computing policies and practices**.

Below is some information on common security risks, threats and vulnerabilities associated with social media tools. It is important to remember that the social media capabilities and uses are evolving constantly, as are the technologies and devices available to the public in a highly competitive market. In addition, individual social media sites, such as Twitter and Facebook, make changes to their settings. Within this changing environment, computer hackers continually devise new methods to outpace the technology and meet their objectives. New security risks, threats and vulnerabilities emerge on a regular basis, therefore, security risk assessments on social media in use by the B.C. government must be updated to meet these challenges.

Following are some of the most common security risks and threats to consider:

Identity Theft or Identity Fraud is the goal of cybercriminals in seeking out personal information – to use a person's credentials (user name and password), personally identifying information (driver's licence, social insurance number, personal health number), and financial information (credit and debit card numbers and PINs, bank account numbers), as well as the identity and personal information of their contacts.

Phishing: Phishing involves a fraudulent e-mail urging the recipient to go to a website by clicking on a link, video or attachment. The e-mail will usually appear to be from a legitimate source, but once the user complies by clicking on the link, video or attachment, their information can be captured. The cybercriminal can install malicious code on their computer and obtain access to both the computer and the information it contains, including the contacts list.

Spear Phishing: Spear phishing is an attack that targets a specific user or group of users by sending a phishing e-mail to catch their specific interest, and attempts to deceive the users into performing an action that launches an attack.

Posting Sensitive Information: The lines between private life and work continue to blur as people use computers and mobile devices for information gathering and communication in both areas, and in between. As employees use the same Internet and social media tools in both places, they might inadvertently publish information considered sensitive by the employer. The information from one employee may not be sufficient, but added together can reveal a corporate picture that can be used for social engineering (i.e. getting people to give important information voluntarily, because they believe that the other person is trustworthy) or for brute force attacks.

Viruses and malicious code (malware): Cybercriminals design viruses that will "fool" anti-virus programs, target social media tools, steal the personal details of the user and his or her friends or contacts, and send them e-mails containing malware or inappropriate content. By planting malicious code or malware on a person's computer, a cybercriminal can gather information about the user, record everything that is typed (including user names and passwords), and even take control of part of the computer to use for their purposes without the user's knowledge.

Spam and Internet Hoaxes: With postal mail, these are called "chain letters" or "junk mail". They involve e-mails that encourage the recipient to forward the message on to the people they know. The e-mails can contain malware that will capture information, or request the recipients to take action, with the outcome being of benefit to the cybercriminals that generated the e-mail. It is estimated that as much as 90% of e-mails world-wide on any given day are Spam.

Insufficient Authentication Controls: With many users or contributors on a site, there is a risk that one individual could make a change that negatively affects the overall system.

Weak Password Rules: Contributors to online sites, including social media tools, often use passwords that are easy to guess (the most common being "123456"), or have password-reminder questions that are unsafe because the answers can be found online (their pet's name, etc.). Using the "remember me" or "remember my password" feature is a security risk because the information is stored on the Internet.

Insufficient Anti-Brute Force Controls: Lack of sufficient protection enables attackers to guess the users' or administrators' passwords, often due to the use of the "remember me" function, and lack of protection from brute force attacks on logout.

For readers with a technical background, the following security vulnerabilities are associated with social media tools: clear text passwords, cross site scripting (XSS), insufficient limits on user input, cross site request forgery, and information leakage.

What to Consider if Social Media will be a Part of your Program or Business Area

Your first point of reference should be the document *Guidelines for Conducting Public Engagement, Specific to Social Media* which outlines a number of key areas of policy and legislation that need to be complied with when using social media tools. All employees must read and understand those guidelines before conducting government business on any social media sites. They provide clear instructions, including important privacy considerations with regard to the collection and disclosure of personal information, as well as information on intellectual property and records management. Employees must also read this document, which provides a much more detailed information security perspective.

Managers need to be aware that the risks of using social media are a reality, and they will grow and evolve as the cybercriminals and hackers develop new ways to disrupt business, steal credentials, grab personal and sensitive information, and basically cause a lot of damage.

Following are some important Tips for Managers:

- Ensure you and your staff have read and follow the *Guidelines for Conducting Public Engagement, Specific to Social Media* document
- Ensure that employees understand that when they are posting information to a public social media site, they are posting it on the Internet. Once information is on the Internet, it cannot be amended, deleted or retrieved.
- Ensure that employees are aware of the BC government's Information Security Policy.
- When you create your Social Media account, make sure you consider which security settings provided by the site are best suited for your situation and that you understand the terms and conditions of use on the site.
- Think about your requirements regarding the integrity and availability of information you want to share. Remember, you may be using a site that is not controlled or managed by government. Can you live without the information if the data, or the site, is unavailable for a short period of time, or lost forever? What security controls exist for access to data on the system and will you be able to ensure data provided by one person cannot be altered by another? Will you have the privileges you need to edit (remove or change) your postings?

- If you have questions or concerns regarding your information security requirements, contact your Ministry Information Security Officer who can assist you with assessing risks and selecting appropriate security controls. They can also work with you to determine if a Security Threat and Risk Assessment is appropriate for your initiative.
- With the adoption of social media tools, it is even more important that employees know and follow the guidelines on the Appropriate Use of Information Resources in the Core Policy and Procedures Manual. While employees are trusted to use social media tools appropriately, they can inadvertently use them in a manner that violates the guidelines and find themselves part of a security investigation, which is only one of the potential consequences.
- Employees must immediately report any suspected or actual information incidents (potential or actual breaches of security) to their supervisor or manager, and immediately notify the Office of the Chief Information Officer by dialing the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866-660-0811 and selecting Option 3. You will then be contacted shortly by the OCIO's Investigations Unit which will seek further details. This procedure is outlined in the Information Incident Management Process which was developed by the B.C. government.

Tips for Social Media Users to Mitigate Associated Risks?

Research into security and privacy breaches world-wide has consistently shown that many of these incidents can be avoided through security education and awareness. If the users know how to protect information and the technologies they use, through proper computing behaviours, they can play a significant role in mitigating risks and preventing security and/or privacy breaches.

Prior to using social media tools in the workplace, following are some important tips for computer users to know that do not require advanced technical knowledge. These tips apply both in the workplace and for personal use outside of work.

- Be aware that individuals online may not be who they claim to be.
- Be familiar with and configure the security and privacy settings to protect your user profile and information on any social media site, and be aware of changes made by the company.
- Assume that information posted on a social media site is on the Internet, even if you have restricted it to certain users (cybercriminals have been able to work around some of these settings).
- Know the reputation, terms of usage agreement (read them before clicking Agree), and the security risks before you start using a social media site.
- Verify the URL (web address) of social media sites before registering and contributing material.
- Use strong passwords to secure your social media accounts and change them every 90 days.
- Do Not use the same user name and/or password as you do for your government account (i.e. IDIR).
- Do Not use the "remember my password" or "remember me" feature, as this information is stored on the Internet and is retrievable by someone with the knowledge and skill.
- Watch for changes in your profile that you did not initiate. If you spot unauthorized changes, immediately change your password and contact the site administrators.
- Restrict your use of online applications (software programs) and do not run or download applications from an unknown source, especially if it is sent to you unsolicited.
- Report any online harassment, stalking or threats of harm to your manager and to the local police.

Social media tools present exciting opportunities for communication and engagement within government, and between government and the public. The tools are there to enhance our work and create new opportunities for the way that government delivers its programs and services. At the same time, it is essential that all personnel are aware the security threats that come along with social media tools and that they follow the guidelines provided to them to ensure the protection of information.

Questions about social media in the workplace? Please e-mail citizenengagement@gov.bc.ca, or to read the Guidelines: http://www.gov.bc.ca/citz/citizens_engagement/index.html

Questions about information security? Please e-mail CITZCIOSecurity@gov.bc.ca

Sources:
BC Government's *Guidelines for Conducting Public Engagement, Specific to Social Media*
Secure Enterprise 2.0 Forum - *Top Web 2.0 Security Threats, 2009 Industry Report*
CIO Council - *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*
Information Security Forum - *Blogging and Social Networking- a Guide to Potential Dangers*
U.S. Environmental Protection Agency Guidance - *Representing EPA Online Using Social Media*