Revisit Internal Policy for Changing Social Media Rules

By Sean Colicchio - CISSP, CEH

May 2013

White Paper

essextec
GETTING IT DONE TOGETHER

INTRODUCTION

Can financial organizations have a fully mature risk management program without a social media specific focus? Not according to newly proposed guidelines from the Federal Financial Institutions Examination Council (FFIEC). In January 2013, the FFIEC proposed new guidance to regulate social media based activities in which banks and credit unions participate. Once approved, these new guidelines will affect all organizations governed by the Consumer Financial Protection Bureau (CFPB).

Social media channels provide intriguing new business opportunities. However, social media channels also expose organizations to new risks. Earlier this year, the Associated Press was the victim of a targeted phishing attack that used the tragic Boston bombings to coerce email recipients into clicking a link in an email. Although the email victims were able to view the video in the email, they also unknowingly allowed the attackers to gain "back door" access to their system. Once access was granted, the attackers could harvest any information that was on the system - including stored credentials. One of the credential sets was of particular interest to the attackers: the authorized AP Twitter account. The attackers sent out a fake tweet to the world and created a hoax that briefly affected the global economy. The fake tweet went out and the Dow Jones Industrial Average temporarily became sharply lower. The Dow fell approximately 150 points after the bogus Twitter posting. A simple click of a mouse by an unknowing AP employee caused an economic plummet. Risk must be considered when implementing a social media plan.

Although the social media strategy should be strong enough to stand on its own, it must be formed with the organization's existing objectives in mind. A properly executed social media plan can have a wealth of benefits, including updates on products and services, education of the customer around an organization's value, and informing clientele of changes in the industry. The upcoming regulation changes indicate that updates to internal policy must take place for the majority of financial organizations, and any informal social media campaigns must be formalized, documented, and revisited to ensure that aspects of governance specifically address social media. They define these mandates as any form of communication on the Internet through which content can be shared. There are fundamental risk management strategy components that should be considered to ensure that organizations are sufficiently prepared for these upcoming changes.

A properly executed social media plan can have a wealth of benefits

cfpb

Consumer Financial
Protection Bureau

STEPS TO SOCIAL MEDIA COMPLIANCE

There are several concerns that organizations should address when trying to adopt a risk centric social media program. Here are steps that financial institutions can take to prepare for social media compliance with the approaching directive.

1. Create a Social Media Team

This team will develop the organization's social media program. An effective risk management strategy includes social media incident awareness. Because social media activity can affect such a wide range of departments and functions, representatives from each department should first be brought together to tackle the potential issues. Create a team that is comprised of all of the departments that could possibly be affected by social media incidents. This team should contain senior members of human resources, legal, IT, marketing, risk management, public relations, compliance, audit, and any other potentially affected departments.

2. Set Social Media Goals

To ensure that the social media program aligns with the organization's strategic objectives, specific goals should be agreed upon as a logical first step. Each department representative should report how it uses social media today and how it plans to leverage it in the future. It is easy for an organization to create a LinkedIn or Twitter profile without first thinking about the purpose. The newly proposed guidelines include quantifying the return on investment of a social media program so it is important to have clearly defined objectives to measure the success of a social media presence.

3. Perform a Risk Assessment

Once the organization has determined how it will use and be impacted by social media technology, it is essential that a formal risk assessment be performed. Based on the probability of an incident and potential reputational damage of social media risks such as an insider threat, consider the inherent risk before researching safeguards and controls. A risk based assessment should prioritize the present risk of social media threats to determine the appropriate level of training, controls, and testing necessary for an effective social media program. The result will help control the residual risk of social media.

4. Draft a Social Media Policy

Once the current risks of social media technology are determined, a social media specific policy should be created to incorporate the concerns and possible control weaknesses within the environment. The policy should be easily accessible by all employees and address the following core areas:

Appropriate Employee Use

Defining what is and what is not acceptable social media use is a large part of the social media program. The social media policy should include which individuals are permitted to post or broadcast content on behalf of the organization. These may be roles that are assigned to this responsibility or a certain individual who has the proper authorization. However, if the organization decides to assign this task, it should be documented and approved by senior management. Establishing this policy not only directs employees, but is also an instrument to exhibit regulatory compliance.

Human Resources

Social media can be a valuable tool used by the Human Resources Department during the hiring process. Note though, the competition is also perusing the content that an organization is broadcasting to potential employees. This understanding can mitigate reputational risk that stems from using social media.

Information Security

The policy should outline any applicable technologies that the organization may use in conjunction with its social media strategy. Incident response is also a major social media concern. Social media produces immediate, though not always calculated, responses. Taking the time to analyze the risks and build a response plan with dedicated team members can make the difference between a small mistake and a long lasting negative public perception.

Even if no social media presence exists, organizations should be prepared to speak to negative comments or posts that arise through social media channels.

Marketing

Quality content will last a long time, so organizations investment in content marketing will remain relevant for potentially many years.

Moreover, great content marketing will also earn significant “earned media” whereby users and other media outlets may talk about and share content to millions more users - potentially producing millions of dollars in free brand exposure. A return on investment is being reviewed by FFIEC proposed mandates, so marketing departments should be concerned with making a positive impact.

Vendor Management

FFIEC has listed third party due diligence as a requirement when considering social media technology vendors. At the very least, the existing vendor management policies in place within the organization should be expanded to include social media.

5. Create a Content Definition and Change Management Process

The type of content that will be pushed out over social media channels differs greatly depending on the purpose of the social media program.

The social media program should include what is not acceptable for the organization to broadcast. These pieces of information should include private customer information, negative language, any trade secrets, and intellectual property secrets.

6. Educate and Enforce

The FFIEC guidelines include formalized training for employees surrounding social media policies and procedures. Industry best practices dictate comprehensive initial training, regular interim training, and training whenever the technology, policy, or procedures change. Although the social media team needs to be adequately trained, training should reach all employees because anyone can affect the social media program.

No policy can be effective unless it is carefully monitored, enforced, and revised (*i.e.*, maintained) if necessary. Organizations should assess what defines non-compliance with the social media policy in order to determine the course of action if such an event occurs. It should be clearly communicated to employees that the enterprise takes its strategy, as well as any documented sanctions for violations, seriously. When an audit team arrives to review internal controls, the program should be auditable, repeatable, and able to produce evidence.

> *Because social media affects your entire organization's risk posture, it cannot be the sole responsibility of the marketing department.*

CONCLUSION

Because social media affects your entire organization's risk posture, it cannot be the sole responsibility of the marketing department. The organization's stakeholders need to determine how social media can contribute to the organization's needs without compromising security or legal requirements. By following these key priciples, financial organizations can be ready for social media specific requirements when they are approved.

ABOUT THE AUTHOR

Sean Colicchio - CISSP, CEH

Sean is a trained professional in risk analysis with several years of experience in information and network security. He has a proven track record utilizing a methodical manner to gather, document, and present specific customer needs or requirements. Sean has a strong familiarity with NIST, ISO 27001/27002, FFIEC, NCUA, HIPAA/HITECH, standards, as well as PCI and other industry and regulatory compliance requirements. Sean also possesses a solid understanding of OWASP, OSSTMM, and other security and auditing frameworks. By joining Essex Technology Group, Inc., Sean has been able to couple his experience with that of other risk management professionals and provide secure risk management guidance to organizations, regardless of size or sector. Sean holds several professional certifications regarding security including CISSP, CEH, and Security+, as well as a Bachelor of Science degree in Computer and Network Security.

> Dynamic Infrastructure > Data Management / Analytics > Business Risk Services

Essex Technology Group, Inc.
> 201 West Passaic Street
Suite 303
Rochelle Park, NJ 07662
> exceed@essextec.com
> 1-888-519-1518
> essextec.com

© 2013, Essex Technology Group, Inc.

essextec
GETTING IT DONE TOGETHER