

Information Security Management Handbook

Sixth Edition

Volume 7

Edited by

Richard O'Hanley · James S. Tiller



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

AN AUERBACH BOOK

Information Security Management Handbook, Sixth Edition, Volume 7
Edited by Richard O'Hanley and James S. Tiller
International Standard Book Number-13: 978-1-4665-6749-8 (Hardback)
© 2014 by Taylor & Francis Group, LLC

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2014 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed on acid-free paper
Version Date: 20130723

International Standard Book Number-13: 978-1-4665-6749-8 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

Information Security Management Handbook, Sixth Edition, Volume 7
Edited by Richard O'Hanley and James S. Tiller
International Standard Book Number-13: 978-1-4665-6749-8 (Hardback)
© 2014 by Taylor & Francis Group, LLC

Contents

Introduction.....ix

Contributors..... xiii

DOMAIN 2: TELECOMMUNICATIONS AND NETWORK SECURITY

Communications and Network Security

1 Securing the Grid3
TERRY KOMPERDA

Network Attacks and Countermeasures

2 Attacks in Mobile Environments.....23
NOUREDDINE BOUDRIGA

DOMAIN 3: INFORMATION SECURITY AND RISK MANAGEMENT

Security Management Concepts and Principles

3 Security in the Cloud35
SANDY BACIK

4 Getting the Best Out of Information Security Projects.....45
TODD FITZGERALD

5 Mobility and Its Impact on Enterprise Security57
PRASHANTH VENKATESH AND BALAJI RAGHUNATHAN

6 An Introduction to Digital Rights Management.....67
ASHUTOSH SAXENA AND RAVI SANKAR VEERUBHOTLA

7 Information Security on the Cheap.....81
BEAU WOODS

8 Organizational Behavior (Including Institutions) Can Cultivate Your
Information Security Program 101
ROBERT K. PITTMAN, JR.

9	Metrics for Monitoring.....	121
	SANDY BACIK	

Policies, Standards, Procedures, and Guidelines

10	Security Implications of Bring Your Own Device, IT Consumerization, and Managing User Choices.....	133
	SANDY BACIK	
11	Information Assurance: Open Research Questions and Future Directions	143
	SETH J. KINNETT	

Security Awareness Training

12	Protecting Us from Us: Human Firewall Vulnerability Assessments	151
	KEN M. SHAURETTE AND TOM SCHLEPPENBACH	

DOMAIN 4: APPLICATION DEVELOPMENT SECURITY

Application Issues

13	Service-Oriented Architecture.....	161
	WALTER B. WILLIAMS	

Systems Development Controls

14	Managing the Security Testing Process.....	179
	ANTHONY MEHOLIC	
15	Security and Resilience in the Software Development Life Cycle	197
	MARK S. MERKOW AND LAKSHMIKANTH RAGHAVAN	

DOMAIN 5: CRYPTOGRAPHY

Cryptographic Concepts, Methodologies, and Practices

16	Cloud Cryptography	209
	JEFF STAPLETON	

DOMAIN 6: SECURITY ARCHITECTURE AND DESIGN

Principles of Security Models, Architectures, and Evaluation Criteria

17	Identity and Access Management Architecture.....	221
	JEFF CRUME	
18	FedRAMP: Entry or Exit Ramp for Cloud Security?	239
	DEBRA S. HERRMANN	

DOMAIN 7: OPERATIONS SECURITY

Concepts

19 Data Storage and Network Security251
GREG SCHULZ

DOMAIN 9: LEGAL, REGULATIONS, COMPLIANCE, AND INVESTIGATIONS

Information Law

20 National Patient Identifier and Patient Privacy in the Digital Era259
TIM GODLOVE AND ADRIAN BALL

21 Addressing Social Media Security and Privacy Challenges.....267
REBECCA HEROLD

Investigations

22 What Is Digital Forensics and What Should You Know about It?279
GREG GOGOLIN

23 eDiscovery287
DAVID G. HILL

24 Overview of the Steps of the Electronic Discovery Reference Model.....293
DAVID G. HILL

25 Cell Phone Protocols and Operating Systems303
EAMON P. DOHERTY

Major Categories of Computer Crime

26 Hacktivism: The Whats, Whys, and Wherefores321
CHRIS HARE

Compliance

27 PCI Compliance345
TYLER JUSTIN SPEED

28 HIPAA/HITECH Compliance Overview.....357
JOHN J. TRINCKES, JR.

Index367

Information Security Management Handbook: Comprehensive Table of Contents387

Introduction

This is the first annual edition of the *Information Security Management Handbook* since 1994 without the guidance and the insight of Hal Tipton. Hal passed away in March 2012. He will be missed by a lot of people for a lot of reasons.

It seems that every year is an interesting one for information security, and 2012 was no different. It is interesting, too, how perceptive Kaspersky Labs, for example, was with its forecast. It also foreshadows the end of online trust and privacy. If you cannot trust digital certificates, what is left to trust?

Kaspersky Cyberthreat Forecasts

2012	2013
Cyber weapons	Government surveillance
Mass targeted attacks	Continued targeted attacks
Mobile threats	Mac OS X malware and mobile malware
Attacks on online banking	Cloud attacks
PPI attacks	PPI threats
Hacktivism	More hacktivism
	Problems with trust and digital authorities
	Ransomware and extortion malware
	Espionage and other government cyberattacks

Cyberwarfare has jumped to the front pages of every newspaper, both print and virtual. Stuxnet spawned Flame, Duqu, and Gauss. While we were all focused on attacks and espionage by China, France, and Israel, Iran mounted a DDoS (Distributed Denial of Service) attack against US banks in retaliation for sanctions that appear to be working. At the same time, Iran’s central bank was attacked. Added to the online attacks is the growing threat of supply chain security, and products shipped with back doors or embedded systems that let them phone home. Witness the difficulty Chinese telecom equipment suppliers like Huawei are having with gaining toeholds in the United States by purchasing the US suppliers.

While Russians and Eastern Europeans are not singled out for cyberwarfare, crime syndicates based there continue to threaten commerce and privacy.

Theft of passwords from LinkedIn and Dropbox, and what seems like daily reports of attacks on or by Facebook show the lure of social media to hackers, and the dangers to the rest of us. And while Facebook and others do not install rootkits like Sony did, its data collection efforts, combined with the apparent insecurity of the site emphasizes the growing dangers of Big Data and the Cloud.

We saw a huge increase in hacktivism as Anonymous and LulzSec launched various attacks on both government and private sites around the world.

It was only a matter of time until Mac OS X became a profitable target. Once critical mass was reached, hackers could not resist investing the time to own it.

As with Mac OS X, mobile devices are becoming even more alluring targets. We have seen the same types of attacks and malware used against PCs adapted to mobile, plus new threats like SMS (short message service) spoofing. Not surprisingly, Android, Google's open platform, has suffered the most. Plus, the growing number of apps for all platforms introduces a level of threat that is hard to estimate, but definitely growing.

M2M and the Internet of Things are creating more opportunities for hackers. From NFC (near-field communication) payments to utility sensors sending unencrypted data, this is a potentially lucrative area for fraud and identity theft. Sensor networks are now in the DIY (do-it-yourself) arena, which creates yet a new class of threats.

BYOD (Bring Your Own Device), IT consumerization, whatever you call it, is making life so much more fun for black hats. It has given new meaning to "insider threats." With portable digital devices being introduced into the enterprise, both with and without permission, we are seeing a manifold increase in threats. Clearly, policies alone are not sufficient to deal with this, and it is unclear how draconian management wants to be with forcing compliance. The products exist, but does the will to use them?

Looking at 2013, the promise of more surveillance, both from governments and online data collectors, means less privacy, even for the most careful users. Short of totally disconnecting from the grid, if such a thing is possible now, it is apparent we do not and would not have privacy.

This edition of the *Information Security Management Handbook* addresses many of these trends and threats, plus new areas such as security SDLC (software development life cycle), as well as forensics, cloud security, and security management. Chris Hare takes an in-depth look at hacktivism, identifying the motivations and the players, and providing advice on how to protect against it. Becky Herold analyzes the security and privacy challenges of social media. Sandy Bacik looks at the security implication of BYOD, and the challenges of managing user expectations. The Smart Grid offers its own security and privacy challenges as Terry Komperda explains. Nouredine Boudriga explains attacks in mobile environments.

There is new guidance on PCI and HIPAA/HITECH compliance. In addition to forensics and e-discovery, a chapter looks at cell phone protocols and operating systems from the perspective of a forensic investigator.

I have heard it said, "You can't fix stupid." So many of these attacks are successful because of clueless or irresponsible users. In what I hope is not a vain effort, Ken Shaurette and Tom Schleppenbach look at human firewall testing, social engineering, and security awareness. We also look at security and resilience in the software development life cycle, managing the security testing process, and SOA (service-oriented architecture) security.

Here is a shout out to my friend Jim Tiller, head of Security Consulting, Americas for HP Enterprise Security Services, for his help in preparing this edition. Jim's done a lot for the Handbook over the years, and I am hoping he will continue.

All-in-all, this is a good volume of the *Information Security Management Handbook*. We are working on the next edition now. If you would like to contribute, please contact me at 917-351-7146 or rich.ohanley@taylorandfrancis.com.

Richard O'Hanley

Chapter 21

Addressing Social Media Security and Privacy Challenges

Rebecca Herold

Contents

What Is Social Media?	268
Benefits	268
Risks	269
Using Social Media Apps	269
BYOD Issues	270
Posting Photos and Videos.....	270
Common Risks and Scams	271
Eleven Topics to Cover within Social Media Policies.....	271
Appropriate Use.....	271
Blogging	272
Wikis.....	272
Information Not to Post	272
Marketing.....	273
Security Controls	273
Time Spent on Social Media Sites.....	273
Linking with Others	274
Posting Photos and Videos.....	274
Reacting to Posts.....	274
Donor Searches.....	275
Summary.....	275

Addressing information security and privacy within business organizations has provided numerous additional challenges with recently introduced technologies (such as big data analytics, the use of personally owned computing devices at work, and cloud services) and comparatively new online habits (such as social networks, the use of always-on location tracking apps, and using the same user IDs for social networks as for work systems) of individuals. Among the many challenges are those that come along with social media use. There are many benefits that can be realized through the use of certain social media sites within businesses, but it is important when planning to take advantage of those benefits to also know and understand the associated risks, both to privacy and to network and information security.

What Is Social Media?

Social media is media that is designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques. Social media uses Internet and web-based technologies to transform the traditional showing of information into an interactive sharing of information. It supports transforming people from content consumers into content producers. Social media is increasingly used for more types of interactions, and is playing significant roles in social, political, and other types of causes.* It is increasingly being depended upon as a source of information, significantly so within the business industry, even though many, and indeed most, sites are far from trustworthy with regard to the accuracy of the information.

A few examples of the commonly used types of social media sites include

- Blogs such as TypePad, WordPress, and so on
- Collaboration sites, such as wikis (e.g., Wikipedia, Delicious) and social news (e.g., Digg)
- Livecasting and meeting sites such as Skype, Livestream, and so on
- Microblogs such as Twitter
- Photography- and art-sharing sites such as Photobucket, Flickr, Picasa, VineMe, and so on
- Presentation-sharing sites, such as Scribd, Slideshare, and so on
- Product review sites such as Epinions.com, MouthShut.com, and so on
- People review sites such as RateMDs.com, Healthgrades.com, and so on
- Social networks such as Facebook, LinkedIn, Google+, Pinterest, and so on
- Video-sharing sites such as YouTube, Vimeo, and so on
- Virtual worlds such as Second Life, Maple Story, and so on

Benefits

When businesses are determining policies for social media use, not only must the risks be considered, but the business leaders must also acknowledge that there are potential benefits to the organization for using social media sites. When used in a thoughtful and risk-mitigating way, social media sites can help to improve your business and business services. The key is to establish social media policies and supporting procedures that not only mitigate the associated risks, but at the same time also support the appropriate business uses. Business organizations, and their business associates and other contracted workers, are using social media to provide beneficial services in many areas, such as the following:

* Cahr, D. What is “social media” anyway? Legally Social, 2011. <http://www.legallysocial.com/2011/02/what-is-social-media-anyway/>

- Customer service
- Knowledge sharing and collaboration
- Patient health education
- Customer awareness
- Learning
- Marketing
- New contacts
- News/world events
- Patient care
- Research
- Crisis management

The information security and privacy personnel must work with marketing, human resources (HR), and other areas of the organization, which are responsible for the listed activities to determine both the risks and the benefits.

Risks

As with any technology, along with the good, there is always the harmful. While there are many benefits, there are also many risks and dangers with social media use, most of which can negatively impact all types of businesses. The following sections list some of the most common damages that have already occurred, some of them many times.

Using Social Media Apps

There are increasingly more apps* being created for social media sites every day. Apps introduce even more risks largely because they are yet another party, a third party, taking information from social media sites and the site users, often in ways the app users do not realize, and then using that information in ways that the associated individuals may not like or want. For example, some currently popular apps and the associated incidents include:

- Foursquare automatic posts have led to physical altercations, break-ins, and other types of crime as a result of people making their posts public instead of restricting them to just those they really want to see them.
- When Spotify came out, a lot of people were embarrassed to have all their music choices showing on the publicly accessible ticker on Facebook. Many had others (such as their friends or family members) who were getting on their computers and purposefully listening to songs that would be displayed as coming from the actual computer owner just as a prank to embarrass them.
- FarmVille and Texas Hold'em reportedly sent Facebook user information to at least 25 advertising and data firms.†
- Until July of 2012, Instagram had a privacy vulnerability that exposed private photos to anyone without requiring authorization.‡

* “Apps” is a shortened common term that has evolved from “application software.”

† Vamosi, R., Protect your online privacy (without reading all the fine print). *PCWorld*, March 30, 2011. http://www.pcworld.com/businesscenter/article/221104/protect_your_online_privacy_without_reading_all_the_fine_print.html.

‡ Ragan, S., Instagram patches privacy vulnerability that exposed private photos. *Security Week*, July 12, 2012. <http://www.securityweek.com/instagram-patches-privacy-vulnerability-exposed-private-photos>.

In August 2012, there were more than 13,000 health, fitness, and medical apps in existence,^{*} and more apps were emerging at an increasingly quickening pace. While some of these are targeted at patients, a large number of them were created primarily for doctors and/or nurses, many of which are meant to be used to prescribe treatment in various ways. Apps are being used to treat health problems such as “diabetes, cardiology, rheumatoid arthritis, and physical therapy—and allow doctors to prescribe apps to their patients.” Physicians can also communicate with their patients using apps.[†]

To properly address information security and privacy risks related to having business workers using social media apps, it is important to determine the following:

- a. What apps are your workers using? Document them.
- b. Are they using apps that are collecting business information, or could be, unbeknownst to your employees?
- c. Are they using apps that are collecting customer information?
- d. Do they even know?

BYOD Issues

It is much harder to address privacy and information security risks when your personnel are using their own personally owned computing devices, commonly called BYOD (short for “bring your own device”) risks. There are some important ways that you can address these risks, though. Your policies can cover what personnel can and cannot do with information about your business, your employees, your patients, and your customers. This includes the types of information that should not be shared on social media sites. It is appropriate that you direct your workers not to post information about work that would negatively impact work. And that they must not post information about coworkers. If you make the policies about your customers, patients, personnel, and business information assets, then they are applicable even when your workers are using their own devices, and outside of your facilities. You need to make sure that you clearly state this within your policies. Some of the basic rules you should create for social media activities include:

- Do not post about work.
- Do not post about coworkers.
- Do not post about customers, patients, or other individuals associated with your business.
- Do not sync or share files between personally owned computers and the organization’s computers/systems.

Posting Photos and Videos

Most businesses have great concerns about having photos and videos taken in their facilities. Hospitals are one such type of business where photos and videos taken within their facilities brings great privacy and compliance risks. They need to address the types of information about customers and patients, in photos, videos, and even comments that their workers can post to social networking sites. If they do not, they may have to deal with a privacy breach. For example, there have been

^{*} Scher, D., Five signs the medical apps industry is maturing. *MedCity News*, Aug. 8, 2012. <http://medcitynews.com/2012/08/five-signs-the-medical-apps-industry-is-maturing/>

[†] Brusteijn, J., Coming next: Using an app as prescribed. *New York Times*, Aug. 20, 2012. <http://www.nytimes.com/2012/08/20/technology/coming-next-doctors-prescribing-apps-to-patients.html?pagewanted=all>

multiple Health Insurance Portability and Accountability Act (HIPAA) violations resulting from the disclosure of patient information online.* However, if a patient wants to take their own photos while in the hospital and then put them online, that is not something that can really be controlled, unless they start including others in their posts. Other types of organizations, in other industries, face similar challenges. These situations need to be addressed. Your social media policies that cover the posting of photos, videos, and other types of images need to include directives that include

- Posting about the workplace, patients, customers, and coworkers
- Posting personal photos, recordings, and videos
- Posting patient, visitor, customer, and consumer images
- Obtaining consent when others are in the images

Common Risks and Scams

Businesses also need to address the many types of risks that social networks present to their organizations, to their customers and patients, and to their own personnel. Here is a list of some of the most common exploits that online fraudsters and criminals use within social networking sites. Not only do these present risks to businesses, their customers and patients, their employees, and their contracted workers' information, along with the company's reputation and legal liabilities, but they can also cause direct harm in a variety of ways to the workers, customers, and patients in their personal lives.

- Clickjacking
- Denial of service (DoS) attacks
- Fake donation sites
- Hackers
- Key loggers
- Malicious links
- Phishing
- Social engineering
- Spam
- Spear phishing
- Spoofing
- Viruses, trojans, worms, and other malware

Eleven Topics to Cover within Social Media Policies

There are at least 11 topics businesses need to cover within social media policies to help protect their business, staff, patients, visitors, and customers from the risks presented by social media use.

Appropriate Use

Be sure to clearly define the appropriate use of social networks from all possible locations and devices. The policies should address the information (patient, business, customer, and personnel)

* For example, see Green & Associates, Social media HIPAA violations on the rise, *FindLaw*, June 15, 2012. <http://knowledgebase.findlaw.com/kb/2012/May/629328.html>

that can and cannot be used or posted when at the office, when away from the office, and when using personally owned computing devices. The key is to make the policy about the information. Generally, businesses cannot control how people conduct their personal lives away from the office, or how they use their own computers, but they can specify how patient information, business information, customer information, employee information, and other company information assets can and cannot be used or shared, no matter the location or device ownership.

Business policies should describe the appropriate use of social networks (Facebook, LinkedIn, YouTube, and Twitter in particular)

- From the company's networks
- From the company-owned computing devices
- From networks using personally owned computing devices
- From staff-owned computing devices and/or networks
- From public computers/networks

Blogging

Blogging is pervasive. At the end of 2011, there were more than 181 million blogs worldwide, five times more than there were in 2006.* It is likely that a large portion of business workers also blog. Businesses need to make sure that they have policies that explicitly address blogging expectations and requirements. These are too often left unaddressed. Such policies should detail the types of information about the business, organization, hospital, clinic, patients, customers, visitors, workers, and intellectual property that can and cannot be included within blog posts. Such policies need to make clear that references to others, not just by name but also by description, should not be included in blog posts.

Wikis

There should be policies for wikis as well. Specify the wikis that are approved for posting business and other information, and those that should not be used. Some organizations have posted protected health information (PHI) and other types of personal information to wikis, in violation of not only multiple legal requirements but also in violation of their own company's privacy policies. Typically, this was done not realizing that what they did put the sensitive information out, basically for the world to see.

Information Not to Post

Business policies need to define the information that is considered to be "personal information." No matter what you want to label it, use whatever is appropriate to your own organization. But clearly specify the types of information that should not be posted to any website, such as PHI under HIPAA, nonpublic personal information (NPPI) under the Gramm–Leach–Bliley Act, and the more generic personally identifiable information (PII) and sensitive personal information (SPI) that are used extensively throughout the many worldwide data protection laws, as well as in the

* NM Incite. Buzz in the blogosphere: Millions more bloggers and blog readers, March 8, 2012. <http://nmincrite.com/buzz-in-the-blogosphere-millions-more-bloggers-and-blog-readers>

breach notice laws of at least 50 U.S. states and territories.* Also describe the types of confidential business information that should never be posted online.

Marketing

There are seemingly unlimited ways in which businesses, hospitals, and clinics are using social media sites for marketing purposes. Be sure to create policies that clearly outline how the sites can and cannot be used for marketing. This includes specifying the persons, positions, or departments that are authorized to do marketing on the sites, the types of information that should not be posted in marketing activities, and very importantly, the types of information that should not be collected from social networking sites and then subsequently used for marketing. Too many organizations are taking what they find online and putting it into their marketing communications without obtaining any consent from the associated individuals. It is important to understand that just because information is posted for the public to see on a social networking site does not mean that anyone can take that information and use it in any way they want. The marketing requirements and guidelines should include the following:

- Positions and departments authorized to post
- Types of information acceptable to post
- Types of information that should not be posted
- Directives against taking personal information found on online sites to use for marketing or other types of business activities

Security Controls

Businesses need to implement security technologies, physical and administrative controls, and make their workers aware of the security risks involved in using social networking sites. Appropriate security must be implemented to help keep the threats from social media sites from damaging business activities, customers, patients, business activities, and information. These controls should include, at a minimum, antimalware, firewalls, spam prevention, and data leak prevention (DLP) tools that are kept regularly updated to protect against new social network threats.

Time Spent on Social Media Sites

While it is not feasible in most organizations to simply prohibit all social media use while at work, it is reasonable and recommended that businesses establish the parameters within which workers can, and cannot, use social media sites while at work. Here are some general guidelines to specify

- Time spent on social networks during work hours
- Directives to not use social media sites while with customers or patients
- Requirements for using social media sites at work only for short period
- Requirements that social media use should be restricted to only during breaks

* See the full list, along with links to the actual text of the laws, at NCLS, State security breach notification laws, <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>.

Linking with Others

The topic of communications with coworkers, clients, patients, customers, and others related to the business needs to be appropriately and clearly addressed. Businesses need to be sure they do not overstep what is reasonable in restrictions of what personnel do on the sites. By keeping social media policies about the business and associated information, organizations will have better policies than if they try to restrict activities in general. When it comes to linking on LinkedIn, friending on Facebook, and so on, with customers, patients, and coworkers, provide the following guidance:

- Do not ask for passwords from workers to their social media sites.*
- Specify that only authorized personnel can participate from social media accounts established to represent the organization.
- Do not link, friend, and so on from personal accounts that list the employer.

It is also becoming more common for organizations to not allow their staff to friend, link, or otherwise be connected to their customers or patients.

Posting Photos and Videos

While businesses cannot tell workers what they generally can and cannot post on their personal sites with regard to photos and videos, businesses can, and should, have policies that address what can and cannot be posted regarding business, patient, organization, customer, coworker, and other similar types of information.

With regard to patients and customers who want to take photos and videos with coworkers, doctors, nurses, and other staff

- Ask that they only post images that include the staff with the staff's knowledge
- Ask that they do not include others within their images

With regard to staff postings, include the following in social media policies:

- No posting of patient, visitor, or customer images unless approved by the area responsible for privacy compliance or with a written consent of the patient, visitor, or customer
- No posting of images showing facility entries or other staff unless approved by the area responsible for privacy compliance

Reacting to Posts

Establish policies that cover how workers should and should not respond to posts they see online that are related to the organization, coworkers, business, patients, customers, and so on. Typically, workers should not respond themselves; that could create some legal problems and liabilities for their organization if they are seen as representing the views of the organization. Instead, have policies and

* For more information about requiring employee passwords, see Herold, R., 6 Good reasons NOT to ask for Facebook passwords, *Privacy Professor*, March 23, 2012. <http://privacyguidance.com/blog/2012/03/23/6-good-reasons-not-to-ask-for-facebook-passwords>

procedures requiring personnel and contracted staff to report such posts to the appropriate area in the organization.

Some general directives to consider including in social media policies about reacting to posts about customers and staff include:

- Do not respond directly to negative posts.
- Report the negative posts to the public relations (PR) office.
- Do not argue, defame, or otherwise act negatively in communications with others online.

Donor Searches

There is a growing trend to use social networking sites for health-related activities, such as for organ donations. Health care organizations should establish policies that detail the appropriate ways in which such posts should be made. Include the following:

- Only authorized personnel can post messages for such searches.
- Only authorized personnel can post replies to posts offering organs.

Summary

All types of organizations must address information security and privacy issues related to social media use. Organizations in highly regulated industries will have some additional types of unique issues to address. For example, health care providers will need to protect patient information and maintain HIPAA compliance. The first step to successfully controlling such use, and preventing breaches and other problems, is to

1. Establish comprehensive social media policies
2. Have each department establish supporting procedures that will help them meet compliance with the policies
3. Provide regular training and ongoing awareness communications about this topic

To realize the many benefits of social media sites, businesses must be sure to also know and understand the associated risks, both to privacy and to network and information security.