CHAPTER

6

Social Media Security Policy Best Practices

Best practices for social media are still evolving. In the pure security world, many standards are followed, everything from National Institute of Standards and Technology (NIST) standards to ISO 27001, an Information Security Management System standard. By employing current standards, IT can follow security requirements to secure social media. If you look at social media data as you would any other data stream, you can apply current policy frameworks. For example, to secure communications between the author of your blog posts and the website hosting the blog (assuming you are hosting it), you can enable SSL and require a strong password that gets changed every 90 days. Secure data streams are part of Payment Card Industry (PCI) requirements. If the Marketing department sends data to a vendor, you can secure that communication with e-mail encryption or encrypted file transfer.

But the challenge in the social media environment has to do with the content and destination of outgoing communications, as well as the person who is consuming and responding to the communication. For example, encrypting a blog submitted by an employee will not help your company once it's published publicly. The post may give away company secrets if the employee doesn't know he wasn't supposed to share certain bits of information with the public!

Every company must have policies in place and a framework laid out defining acceptable use of social media. Every organization—from small businesses to governments—need to treat social media policies like IT policies—living documents that guide appropriate use. In this chapter, we discuss social media security policies requirements. Specifically, we cover

- The components of an effective policy
- How the H.U.M.O.R. matrix fits into your policy
- Developing your social media security policy

Toward the end of the chapter, we've also included a sample social media security policy that you can use as a guideline for creating your own policy.

Case Study: Growth of Social Media Policy Usage

In the United Arab Emirates (UAE), 45 percent of the population uses Facebook. The UAE eGovernment has released the Guidelines for Social Media Usage in UAE Government Entities,[1] a progressive move toward implementing a social media security policy. The guidelines provide steps to be taken by the government and addresses issues such as access to social media sites from within government offices, account management, employee conduct, content management, citizen code of conduct, security, privacy, and some other legal issues. The guidelines state: "The main driver behind granting access to employees is to ultimately enhance their work performance and contribute to improving their outputs and deliverables." It recognizes that the lines between personal and professional usage of social media sites are often blurred, making the issue of granting access to one rather than the other difficult. It, therefore, recommends: "Access to social media sites shouldn't be banned. Employees should be held accountable for any improper use of any social media site."

The policy covers a wide array of policy topics, including:

- **Policy controls** These outline appropriate behavior and content guidelines when using social media tools.
- **Acquisition controls** Examples of these are found in the "Access to Social Media Websites" section of the UAE's policy. The controls allow for greater security and privacy settings and greater control of information (such as setting strict authentication measures or managing cookies) when subscribing to commercial social media sites.
- **Training controls** These provide awareness and courses for employees on policy, conduct, and best practices when it comes to using social media tools.

This policy is a great start for the UAE. What the government can do to improve this process is to address policy guidelines for monitoring and reporting. They should also add an incident response policy for when things go wrong. The current policy does not address these key concepts in any detail. As their policy states, however, social media management is an ongoing process, and the UAE will most likely modify the policy as the landscape changes.

[1] Ibrahim Elbadawi, "Three Reasons Why the UAE eGovernment Social Media Guidelines of Are Vital," Government in the Lab (Date: March 11 2011), http://govinthelab.com/three-reasons-why-the-uae-egovernment-social-media-guidelines-of-are-vital/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Government20InAction+%28Government+2.0+in+Action%29.

What Is an Effective Social Media Security Policy?

Defining the content of a policy is the first great challenge. Currently, there are no international standards bodies (such as Institute of Electrical and Electronics Engineers or IEEE) to help with this problem. The government is trying to adapt NIST SP 800-53 Rev 3, which is a government standard on information security procedures, to take into account some form of accreditation for services such as Twitter or YouTube as a network system. As these are hosted services, however, you have no control over them; you have to rely on the administrator of Twitter and YouTube to maintain security protocols.

An effective policy has several main components that take into account the type of services used. Social media platforms are both internal and external, and what type you use will necessarily dictate at least some parts of your policy. Here are the key ingredients that policies should have:

- Any regulatory requirements and legal requirements that social media use could impact
- Managing internal and external hosted applications, including monitoring and reporting tools and techniques and testing and auditing
- Enterprise-wide coordination
- Codes of conduct and acceptable use
- Roles and responsibilities for the Community Manager
- Education and training
- Policy management, reporting, and monitoring

How's JAG Doing?

These key ingredients are missing from JAG's policies. They gave themselves a "Poor" rating for most of these categories. To date, JAG's policies have focused on HR and IT: basic Acceptable Use Policies, Employee Code of Conduct, IT Operations Guidelines, IT Security Policy, Internet Use Policy, and hiring policies. Within JAG's HR policies, training and education do not focus on IT issues or social media issues, and within its IT policies, no social media issues are addressed. The Marketing department has not even put out a public version of its social media policy to state the company's position on social media usage. Hopefully, JAG will improve its score in the H.U.M.O.R. Matrix after reading this chapter and implementing new policies.

Regulatory and Legal Requirements

As we've discussed in earlier chapters, the reasons for needing a social media security policy (or a security policy applied to your organization's social media usage) are very similar to any other policy you may have. Employees need guidelines for appropriate usage. The decades-old acronym PEBKAC—Problem Exists Between Keyboard And Chair—certainly applies to today's new social media environment. A number of legal risks also drive the need for documented policies. Several of these include:

- **Discrimination claims** Employees can say anything over social media that might be attributed to the company. For example, you could have a policy basically saying if employees post things on personal sites that impact other employees or the company, they may get terminated. Discrimination claims can lead to an employee claiming a hostile work environment and filing a lawsuit. Or perhaps a supervisor uses social media to disparage an employee during off hours; this could also cause a lawsuit.
- **Defamation claims** Employees may say things over business or personal social media outlets that impact the company or competitors or even customers. Employers may share too much information, including photos, about other employees that can lead to a lawsuit. Case law has not settled on this as yet. A case was pending in which the National Labor Relations Board alleged that American Medical Response of Connecticut Inc. had illegally fired an employee in 2009 after she criticized her supervisor via a personal Facebook post. The firing prompted a lawsuit based on protected speech under Federal labor laws. The case was settled in early 2011. The settlement called for American Medical Response of Connecticut Inc. to change its blogging and Internet policy that barred workers from disparaging the company or its supervisors. The company also has to revise another policy that prohibits employees from depicting the company in any way over the Internet without permission.[2] This is a far-reaching consequence to their overall policy. The modified policy has to very careful in trying to restrict off-hours usage.

[2] "Company Accused of Firing Over Facebook Post," *New York Times* (November 8, 2010), http://news.yahoo.com/s/ap/20101109/ap_on_hi_te/us_facebook_firing.

- **Confidentiality breach** This risk is probably the most prevalent. An employee shares too much confidential information, leading to regulatory fines or even competitors finding out too much.
- **Regulatory breach** Many regulations also include educational components for employees, detailing what is appropriate to communicate about regulated products, such as financial investment opportunities or claims about pharmaceutical drugs, or about disseminating confidential customer information. For example, an employee might easily share too much patient information over social media in breach of the HIPAA Security Rule regulations, as illustrated in Chapter 4 in the case involving a Twitter post sent out by a hospital employee.

Your policy should address the consequences of giving out proprietary and confidential company information; making discriminatory statements; and making defamatory statements regarding the company, its employees, customers, competitors, or vendors. It should address how employees can use the company name and what information can be shared. You need to have a well-documented escalation procedure to apply the right enforcement capabilities, create a framework for chain of custody, document all types of legal discovery and proceedings, and provide justification for possible actions against employees, hackers, or other malefactors. Much social media content is beyond the company's direct control so policies and procedures have to suffice where technology tools cannot have an impact.

Managing In-house (Self-hosted) Applications

Your social media security policy should detail security requirements for using social media sites that you do have control over. Companies that build their own policies and apply their own requirements without the benefit of adopting a secure process for developing applications are developing policies based on how technology and privacy of data has been historically treated in typical security infrastructures. Many approaches to securing a social media application or website are similar to securing your company's ecommerce site or proprietary applications. Differences occur when you are compromised by an employee saying something inappropriate, a customer attacking your company brand, or your sales team losing customer data over social media channels. These problems make it into the public sphere much quicker; customer feedback is almost immediate; and your brand can suffer damage within the span of a few hours.

When using social media sites that you *do* have control over, such as your own WordPress-based Blog or wiki site, key security requirements must be baked into the availability of the sites to your employees:

1. Ensure that you have followed a security assessment process to test applications for risk due to traditional attacks, data management problems, and secure coding practices. Your security processes should detail the basic steps you have to follow in testing a web-based social media application:
   a. Information gathering, including application fingerprinting; application discovery; spidering and Googling; analysis of error code; SSL/TLS testing; DB listener testing; file extensions handling; old, backup, and unreferenced files

   NOTE

   For detailed technical security analysis of secure software testing, review Hacking Exposed 6: Network Security Secrets & Solutions *by Stuart McClure, Joel Scambray, and George Kurtz (McGraw-Hill Professional 2009).*

   b. Authentication testing, including default or guessable accounts, brute force, bypassing authentication schemas, directory traversal/file include, vulnerable remember password and password reset, logout and browser cache management testing
   c. Session management, including session management schema, session token, manipulation, exposed session variables, HTTP exploits
   d. Data validation testing, including cross-site scripting, HTTP methods and XST, SQL injection, stored procedure injection, XML injection, SSI injection, XPath injection, IMAP/SMTP injection, code injection, buffer overflow
   e. Web services testing, including XML structural testing, XML content-level testing, HTTP GET parameters/REST testing
   f. Denial of service testing, locking customer accounts, user specified-object allocation, user input as a loop counter, writing user-provided data to disk, failure to release resources, storing too much data in session
2. Address post-deployment testing and consistent testing of your application over time.
3. Identify what key company and customer information should be encrypted during each data management step: creation, transportation, usage, storage, and destruction.

4. Review how authentication steps are handled for third-party applications and APIs; weak or plaintext unencrypted authentication can allow inappropriate access to or theft of credentials.
5. Define strong passwords and how they will be enforced and when they should be changed, especially if multiple employees in, for example, Marketing might have access to the company account on sites such as YouTube or Facebook.
6. Address log management issues. Where possible, you want to log which employees access the social media corporate accounts and know who posts information. Log management can be extremely important to incident response plans.

In-house Social Media Site Checklist

Once you have built your self-hosted site, follow the approval process for deployment to production, just as you would for any other IT application being placed into production.

Answer these questions to ensure you are meeting the key requirements for approval:

- Are appropriate disclaimers in place?
- Is ownership of the site clearly defined and displayed?
- Is an operations process in place for site update and content review?
- Does content get signed off by appropriate management? Are policies in place for user content moderation?
- Are all users and administrators of the application trained in appropriate usage, moderation, and content creation?
- Have you developed a community manager process?
- Are security testing plans in place to test the application's functions as well as the operating system's and network layer's capabilities to defend against hacker attacks?
- Is an incident response process in place for application usage as well as potential damage to the application's functions?
- Are operations staff assigned responsibilities for maintaining the site?

Managing Externally Hosted Applications

Third-party cloud applications cannot be handled in the same manner as your own infrastructure applications. You have minimal impact on these third-party companies and their security requirements, and influencing them to modify their security posture will probably not be effective. Alternatively, reliance on your own controls is essential. Examples of internal controls to consider include:

- How your employees use these third-party social media sites
- What data is allowed
- How you will monitor your corporate activity
- How you will respond to an external incident

Another key change in how you manage data is that you have to rely on third-party platforms to conduct their own security testing of their applications, and then they may or may not show you the results. You inherently trust these platforms and related applications to keep all the private messages you receive from your Facebook Fans secure from hackers and you rely on third parties not to sell customer lists of your Twitter followers. But has your company asked Twitter or Facebook for a SAS 70 II audit report (which is a third-party analysis of a company's security posture)? As of last year, Twitter agreed to share all public tweets since its inception (2006) and archive them in the Library of Congress—with the exception of deleted tweets. Google already indexes tweets in real time. Yahoo! and Microsoft get copies, too. This could be part of your audit processes. Have you any idea what their security policies are over the data you share with these third-party companies?

The policy framework has to take into account the following major security concepts when dealing with a third-party application:

- Social media is generally based on third-party "cloud" applications and, therefore, your company can't control their security.
- Social media web applications and downloadable applications have the same security challenges as all other web-based applications and other installed software applications.
- The general public is as involved with your company's use of social media as you are, and your policy has to give guidance to your employees on how to handle public interactions.
- Your company should have a public version of your social media policy that explains your positions on social media.

- Sharing of data is a must in social media, but data sharing is also a key aspect of attacks from both a technological hacking perspective as well as a content perspective.
- Malicious code is easier to share via social media portals and downloadable applications that can then connect back to the corporate environment to introduce viruses, Trojans, and other malware.
- Reputation management is often more important than secure technology-based controls when addressing the risks due to social media.
- Enable encrypted communications to the social media site when possible. This is not easy with most sites, but applications are available that can help with this task. One example is HTTPS Everywhere from the Electronic Frontier Foundation (https://www.eff.org/https-everywhere). As the site says:

> HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites. Many sites on the Web offer some limited support for encryption over HTTPS, but make it difficult to use. For instance, they may default to unencrypted HTTP, or fill encrypted pages with links that go back to the unencrypted site. The HTTPS Everywhere extension fixes these problems by rewriting all requests to these sites to HTTPS.

When you install the HTTPS Everywhere add-on in Firefox, it forces encryption on the sites it covers. In Figure 6-1, you see that going to Facebook without HTTPS Everywhere leaves the website unencrypted. Once you install HTTPS Everywhere, you will see, as shown in Figures 6-2 and 6-3, how the "https" is now forced without any user interaction for social media sites you visit.

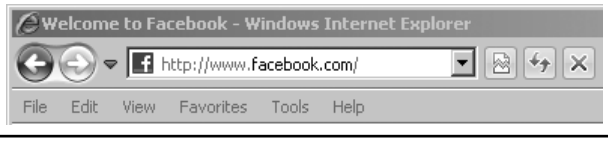

Figure 6-1 *Visiting a site without HTTPS Everywhere turned on and no encryption*

Figure 6-2 *"HTTPS" is forced when visiting Facebook with HTTPS Everywhere.*

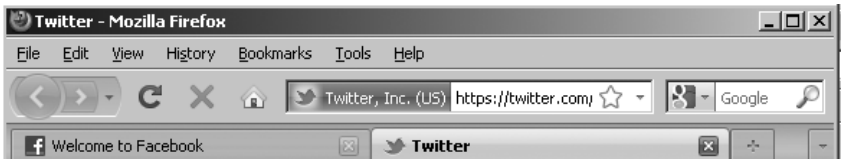

Figure 6-3 *"HTTPS" is forced when visiting Twitter with HTTPS Everywhere.*

HTTPS Everywhere actually offers protection against Firesheep and the software currently supports other sites such as Google Search, Wikipedia, bit.ly, GMX, and Wordpress.com blogs, and, of course, Facebook and Twitter. (As we mentioned in Chapter 5, BlackSheep can also help identify the Firesheep threat.) As Facebook and Google and other sites make HTTPS connections more readily accessible and a default option, the threat of unencrypted communications will decrease.

Externally Hosted Social Media Site Checklist

Although determining the security measures employed by a third-party site may seem difficult, follow at least a minimal set of baseline standards when allowing your company to utilize any website for marketing campaigns, storing customer data, and communicating with the public. At a minimum, you should attempt to gain a better understanding of the third-party application you are using and ask pointed questions to gain insight into its security protocols. Your policy for gathering information should list, at a minimum, these requirements:

- Review the social media site/platform's SAS 70 II audit report. If the site doesn't have one, ask for one to be conducted and get the results sent to you if possible.
- Ask for and review a basic financial summary of the company: Are they profitable or on the road to profitability?
- Review the site's privacy policy for any steps that may compromise your data or your customer's data.
- Ask for the guidelines the site has for its own internal testing procedures for vulnerabilities and review their procedures. What is the schedule for conducting testing?

> ***NOTE***
>
> *In May 2010, the security company F-Secure discovered a malware attack being run by fake Twitter accounts on Twitter posts with the message "haha this is the funniest video ive ever seen." When users clicked it, a Trojan was installed on their systems! If Twitter had a very proactive security program in place, they would have found this before F-Secure.*

- Ask for and review the site's incident response program.
- Review the encryption of the site's data storage, data transmission, and authentication.
- Ask for and review the site's backup strategy.
- What happens to your data if the company goes out of business? This is a question you will probably not get a good answer to, but you may want to ask about a data escrow service.
- Review any documentation the site has regarding industry regulations or types of data stored. Review the site's data breach notifications policy.
- Review the service level agreement with the site. If the site does not have one, ask for one to be developed.

Enterprise-wide Coordination

Like your current human resources policies and IT security policies, your social media policy has to be a companywide program. If only the Marketing team is subject to the policy, other employees will not know what is allowable and will most likely post inappropriate information. If the IT department is the only one following the policy, other departments will not know how to use social media sites in a secure manner or will not receive any training on what can and cannot be posted about the company.

Writing the social media policy is a collaborative effort. Creating more granular social media security policies and educating employees must be a companywide effort. The policy can either be broken down into multiple policies and written as the business functions change, or it can be written in a more generic format to address future changes in related processes, which might be a bit more difficult to do. Most companies currently have a Laptop Policy and a Mobile Device Policy; these are granular policies. The approach you select really boils down to an individual choice. If you do want to write granular policies, you may consider starting out with these:

- Social Media Policy
- Social Media Security Policy
- Employee Code of Conduct for Online Communications
- Employee Social Network Information Disclosure Policy
- Employee Facebook Policy
- Employee Personal Social Media Policy
- Employee Twitter Policy

- Employee LinkedIn Policy
- Corporate Blog Policy
- Corporate YouTube Policy
- Social Network Password Policy
- Personal Blog Policy

Codes of Conduct and Acceptable Use

For any of the policies you define, there are basic requirements that all employees should adhere to and understand. Any HR professional will know these by heart! Widely used examples of such policy provisions include:

- All employees must take responsibility for knowing the policies, just as they do for reading the company handbook. Training is, of course, a requirement to ensure employees can follow the policies properly.
- Employees must understand the policy is global for all social networking activities.
- Employees are under the same confidential restrictions regarding company information no matter what platform they use.
- Any information disclosed publicly should include the appropriate disclaimers, for example, employees should clearly identify themselves as company employees when speaking about the company or about the industry.
- The employee cannot infringe on company trademarks or intellectual property whenever communicating outside the company.
- Guidelines about sending out certain types of company-related information, from brochures to sales proposals.
- Employees can be terminated for inappropriate use of company information or conduct unbecoming an employee that negatively impacts the company.

When different departments collaborate on developing policy and managing technologies, a company can get a better handle on how social media will be used internally and externally and how rules for social media usage can be developed. Here are some basic rules and guidelines that employees must follow:

- Employees must read and understand all policies related to social media.
- Employees must understand they need to be trained appropriately in social media usage.

- Employees may use company resources only for approved social media activities during working hours.
- Employees must not disseminate confidential information.
- Employees should not use nonsecure social media systems to conduct company-related work activities, unless otherwise specified.
- Employees are not allowed to circumvent company security procedures and technologies.
- Employees should not share login information to social media sites in any unapproved manner.
- Employees will follow company guidelines on using secure passwords.
- Employees should understand they represent the company when they discuss the company name on social media sites and will respect company policies.
- Employees should have, at a minimum, yearly training on security processes.
- Employees are responsible for security along with the IT department.

Roles and Responsibilities: The Community Manager

The Community Manager is a relatively new role as applied to the online environment in Web 2.0 and beyond. Where the role fits into the organizational structure is still up for debate, and largely depends on the company's industry, culture, and objectives for participating in social media. In many companies, the Community Manager role is a Marketing function due to the overwhelmingly communicative nature of social media. Other companies, such as Comcast, use social media primarily for improving customer service. Lego, the toy manufacturer, uses social media for new product idea generation. Dell has successfully used social media for community building and sales promotions. Dell encourages *all* employees, regardless of department, to engage with their communities via social media. Employees spend an average of 20 minutes/day connecting with online communities and customers.

Some companies have recognized the cross-functional nature of social media, setting up a separate reporting line as a cost or a profit center or as a shared support service, based on strategic objectives. Whichever the case, the manager guides strategic, tactical, and operational activities related to social media outlets and implements daily procedures, plans, ad-hoc campaigns, and oversees resources and processes around multiplatform community scalability.

The role must be defined at the outset from the standpoint of secure utilization of social media, however. Part of the Community Manager's responsibility involves interfacing with the IT Security, Legal, and Human Resource departments to ensure a cohesive strategy that reduces risk to the company from the potential social media threats discussed in Chapters 4 and 5.

The current role of the Community Manager usually involves a combination of the following:

- Welcoming customers to the organization's social community
- Identification and relationship building with key influencers
- Real-time monitoring, moderating, responding to, and redirecting conversations
- Encouraging interaction and community development among members
- Managing programs and content
- Managing internal resources allocated for social media
- Enforcing policies and guidelines
- Managing tools for social media development programs and communications
- Reporting on activities and developing new metrics
- Tracking customer sentiment
- Developing, implementing, and managing content creation strategy
- Managing responses to the brand
- Delegating feedback to internal teams
- Developing web communications to optimize all customer interactions
- Managing the company blog for engagement and readership
- Responding to and managing crises
- Developing internal communications through thought leadership, employee engagement, and training
- Online and offline event planning for connecting the company with its community of customers and clients and providing forums for like-minded consumer advocates to meet and interact

Nowhere in this description is there an explicit interface between the Community Manager and the IT, Legal, and Human Resource departments. This integral connection is too often overlooked in policies and by management. The role of the Community

Manager must expand to take on a liaison project management function that goes beyond just managing social media content and communications. To be effective as a real interface for the company, the Community Manager's role must take on these further responsibilities:

- Coordinate policy development among all business units.
- Work with IT Security to track incidents.
- Work with Marketing and IT together to coordinate public response to incidents or customer threats.
- Work with Legal to understand application laws to social media usage.
- Work with Human Resources to ensure all employees involved in social media understand the restriction on usage and potential dangers.
- Work with IT Security to use appropriate tools to track, monitor, and report on employee use of social media tools.

These new tasks take the Community Manager out of his or her current role. A best practice would be to designate someone in IT or IT Security to partner with the Community Manager or even take on some of the Community Manager's responsibilities in the IT realm. In the role of assisting the IT department with helping employees understand the security implications of social media, the Community Manager can share responsibility with IT for reviewing and searching for security information related to the social media tactics being used. This has to be a shared responsibility, as social media site monitoring includes:

- Reviewing company profile pages daily to determine if any inappropriate or hacked content has been displayed
- Reviewing other sites and profiles referenced or relevant to the company for acceptable use of company information
- Creating a routine for checking to see if users and customers connected to the company's social media profiles are conducting their online activities in accordance with company acceptable standards of association
- Scanning links to the company to see if any compromised pages have been posted
- Working with IT Security to test company sites for weaknesses
- Working closely with IT Security to review what new vulnerabilities might impact applications and websites used for social media marketing campaigns

TIP

Sites for tracking vulnerabilities include the National Vulnerability Database (http://nvd.nist.gov/nvd.cfm), Security Focus Database (http://www.securityfocus.com), and Open Source Vulnerability Database (www.osvdb.org). On these sites, you can search for technologies and social media channels you use for any known vulnerabilities that might compromise your security.

The successful implementation of the Community Manager role has to be assessed by multiple departments. IT must be able to communicate technology challenges, threat scenarios from social media, and response capabilities. Human Resources must be able to implement and enforce policies through the assistance of the Community Manager, and together, they must work with employees to enforce compliance with policies. Marketing must be able to coordinate communication projects and business objectives to all other departments through the Community Manager and have access to the right technology resources to accomplish its goals. Legal should be able to coordinate regulatory restrictions on social media usage across all departments through the Community Manager.

With these new responsibilities, the reporting structure will be a challenge, particularly as the role naturally evolves cross-functionally over time. Although an employee should never have two bosses, which is often a recipe for failure, involving other departments in a goal setting process for evaluating the Community Manager's job performance can be effective. The Security Director has a key role to play in working with the Community Manager. A number of security technologies, which many large companies already have in place, can also be applied to secure new media communications. Data loss prevention tools are probably the most comprehensive for monitoring the types of data coming into and leaving the company's environment. By putting a process in place for IT Security to work with the Community Manager, new projects and campaigns, new web applications, and proposed social media tools can be monitored, tracked, and reported on in a more timely manner.

Education and Training

As with any security framework, educating your staff is paramount. A good baseline training program can reduce risk as well make employees less likely to cause inadvertent breaches. Employees can be unaware of how easily social media channels can be used to manipulate users into divulging confidential information or granting computer

system access. Using social media, attackers try to use a variety of techniques (just a few a noted here) to gather private information:

- **Pretexting** Using an invented scenario and a piece of known information to establish legitimacy in the mind of the target. Information is then typically used to try to obtain Social Security numbers, date of birth, or other personal verification measures.
- **Phishing** An e-mail that appears to come from a legitimate source (like your bank) requesting verification of information and warning of a consequence for noncompliance.
- **Trojan horse** A destructive program that masquerades as a benign application.

Many employees recognize some of these attack techniques. Unfortunately, not every employee understands the complete attack landscape, which can leave your company and possibly your network vulnerable to attack. Employees need to understand the importance of network security and the key role they can play in helping protect company information. For example, employees may create common passwords to use on social media sites to simplify their interactions and daily status routines, but this ease-of-use scenario can also make it simpler for the attacker to gain access to their social media accounts and possibly leverage further attacks into your network.

The benefits of employee security training include:

- Employees absorb the importance of "best practices" and then they can, in turn, practice and preach a broader understanding of a company culture of safety and security.
- Employees are less likely to fall victim to attacks and expose your company to additional attacks.
- Employees learn a new model of acceptable behavior and culture within the company.
- Employees learn about their responsibilities to help prevent malicious activity and detect problems.
- Training helps reduce the risk of intentional or accidental information misuse.
- Training provides a baseline of compliance for federal and state regulations that may require security awareness training.

Policy Management

Once you have your social media security policies in place, you have to update them continuously. The challenge with social media, as compared to other technologies, is the speed at which the sites, technologies, capabilities, and processes change. New functions are being built so rapidly that a completely new capability, function, or application might be available in six months that is not currently covered by your policies. Securing these new functions and understanding how employees and customers interact with new sites is going to require more diligent updates of your policies than you are used to with normal IT security policies.

Both the IT staff and the Marketing staff must have a process in place for researching new technologies, determining what employees and customers are using, and understanding how these new sites affect the company's assets and resources. For example, geolocation is rapidly rising in popularity with new applications coming out weekly, but most companies have yet to grasp the true capabilities, dangers, and opportunities of geolocation applications. To keep abreast of the latest trends and functions, the Community Manager must work with Marketing and IT to

- Select specific sites to read and research such as Mashable.com and TechCrunch.com.
- Review employee web surfing to look for what is trending.
- Put a process in place to analyze new applications before the company is swamped with something unexpected by employees or customers.

H.U.M.O.R. Guidelines

In Chapter 2, we outlined some basic policy questions that you must address regarding your company's overall social media security strategy. Within the H.U.M.O.R. Matrix, we can also apply policy requirements. In Chapters 7–11, we go into details for each requirement in the H.U.M.O.R. Matrix. Different policy matters have to be addressed for each requirement. Table 6-1 lists the key aspects of social media policy to be captured.

H.U.M.O.R. Requirement	Policy Component
Human Resources	▶ Disseminate policy in an understandable format that is available to all employees throughout the company. ▶ Disseminate a public version of applicable policy requirements for employees and customers. ▶ Develop guidelines for using social media for business requirements. ▶ Assure compliance with all legal and regulatory requirements. ▶ Develop a clear response plan for incident management and public interaction. ▶ Create policies for education and training. ▶ Create policies for restricting access to company private information.
Utilization of Resources	▶ Create policy for clear usage of intellectual property by employees and the public. ▶ Create guidelines for response to theft of intellectual property. ▶ Create policy on writing content and plagiarism. ▶ Develop processes for utilizing the correct technology resources for different social media activities. ▶ Create policy for updating tools as capabilities change.
Monetary Spending	▶ Create policies for identifying business justifications for spending budget on social media activities. ▶ Define budgets for education and training. ▶ Develop process for identifying monetary damage through social media activities.
Operations Management	▶ Develop Operations guidelines for IT, Marketing, Legal, and HR, detailing the responsibilities of each department. ▶ Define enforcement requirements and activities that will be taken by HR and IT. ▶ Define the process for understanding what social media resources will be used and what impact the various cloud services will have on the business. ▶ Create a password policy. ▶ Develop processes for threat management.
Reputation Management	▶ Develop clear process for incident response management. ▶ Identify policy for monitoring and reporting on both employees and customer/public social media activities that affect the company. ▶ Develop processes for controlling reputation monitoring.

Table 6-1 *H.U.M.O.R. Matrix Policy Components*

Developing Your Social Media Security Policy

Once you have determined the key components of your social media security policy according to the H.U.M.O.R. Matrix, you have to actually write it. For each component of the matrix, we go through a number of steps in the following chapters to outline tactical implementation. The first step is to understand the risks your company faces. We discussed threat assessment in Chapter 4 and further in Chapter 5. This section of the book goes through the controls you need to implement with your policies. Your threat assessment should have identified the risks to your tools and the websites you use for social media activities. The intent is to identify risks to your social media activities, understand what could go wrong, and implement mitigating controls based on your documented policies.

The Policy Team

The Community Manager can take the lead in organizing the policy team, or the lead can default to the Human Resources department. Other interested parties may include Marketing, PR, Sales, Business Development, Legal, and Customer Service. This cross-functional team should review each operational aspect of your social media strategy, determine the best possible processes to achieve business goals, develop policies, implement the policies, and respond to the changing landscape. All policies should be flexible and be reviewed every six months due to the changing nature of social media environment. The lead should assign individual roles and responsibilities.

All changes must be made and approved by the policy team. The team will conduct periodic risk analysis to the related business processes that use social media, understand the technologies, and determine what operational changes must be made. The team will be responsible for disseminating the changes and ensuring the appropriate employees know what the policy requires. The policy team will be the liaison to other departments that are impacted by social media usage.

Determining Policy Response

Security monitoring of policy violations naturally requires technology managed by the IT department. Automated processes have to search for employee violations and customer and public interactions that impact the company brand over social media platforms. The policy team can determine what constitutes a violation and develop the associated appropriate responses in coordination with Human Resources. Different levels of risk can be addressed with varying levels of response. For example, Facebook

does allow more information to be posted and an employee can easily and unknowingly install a malware Facebook application that's more dangerous than what you face from your typical Twitter usage, which doesn't impact network resources as much.

A response process must be in place for policy violations and related mechanisms must also be in place to actually monitor for violations. If you are looking for internal employee access, then data loss prevention tools are needed. If you are looking for external incidents, then you might need third-party monitoring services such as ReputationDefender.com. You may assign risk levels to different social media activities and apply appropriate resources based on risk to the organization. Once a violation occurs, a clear process needs to be in place to notify the right resources for a response. A fast response is vital, precisely because the real-time, instantaneous nature of social platforms accelerates the speed at which events get passed along and become viral. A plan identifies possible areas for error, minimizes risks, and provides mitigation guidelines all teams can follow on a 24×7 basis.

The level of authority that response teams have has to be defined. Like your disaster recovery plan, you should test your social media response plan for possible attack scenarios. Possible decisions when addressing violations may include:

- Identifying the issue at hand
- Responding to media inquiries
- Acknowledging the problem and responding to mentions in a timely, courteous, and professional manner on relevant blogs, microblogs, and social networks, particularly when posted by influencers
- Determining employee culpability, if any
- Implementing changes to prevent continued use of the access violation
- Isolating the technology (if any) that have been compromised
- Contacting websites that may be involved
- Recording evidence and logging a timeline of events and remediation steps taken
- Contacting the appropriate public agencies if necessary
- Notifying internal executives and legal counsel

A Sample Social Media Security Policy

Each policy varies depending on company size, industry, regulatory requirements, corporate culture, and level of engagement with customers and the public. Some companies might be more concerned with brand awareness whereas others are more concerned with sales activities. If you are a smaller company, you might not be able to field a cross-functional team from Legal, HR, Marketing, Sales, Customer Service, and IT to manage your social media security tactics: it might all fall on Marketing and IT or perhaps just Marketing. This would dictate a number of different policy requirements. But every company still needs a policy in place if it is to engage with the public in a manner that includes risk reduction tactics.

Here is a basic outline you can follow to develop your own social media security policy.

Social Media Policy Outline

1. Introduction
    i. What is this policy all about?

a. Policy Management
    ii. Company rights to change and update this policy

b. Effective Date

c. Goals
    i. What are the goals of this policy (set guidelines, determine responsibilities, manage reputation, etc.)

d. Purpose
    i. What is the purpose of this document and who does it apply to?

e. Scope
    i. What is the applicability to the policy to technologies and employees, contractors and partners, etc.?

f. Policy Owners
    i. Who manages this policy?

2. How Social Media Is Used
    a. Social Media Channels (Facebook, Flickr, LinkedIn, Twitter, YouTube, GoWalla, Foursquare, etc.)
    b. Social Media Benefits (marketing, sales, customer service, new product development, customer feedback, access to media, partnerships, communications, cost reductions, etc.)
    c. Community Manager Objectives
        i. Who is the Community Manager?
        ii. What is the Community Manager's role?
    d. IT Security Department Responsibilities
        i. Define role of IT Security.
        ii. Identify processes to authenticate and authorize each social media platform.
        iii. Define implementation responsibilities.
        iv. Define reporting responsibilities.
        v. Define monitoring responsibilities.
    e. Marketing Department Responsibilities
        i. Define role of IT Security to assist the Marketing department in conducting their responsibilities in a secure manner
    f. Human Resources Responsibilities
        i. Define role of IT Security to assist the HR department in conducting their responsibilities in a secure manner
    g. Legal Department Responsibilities
        i. Define role of IT Security to assist the Legal department in conducting their responsibilities in a secure manner
3. Social Media General Policies
    a. Advertising
    b. Regulatory Requirements
    c. Community Management
    d. Confidentiality
        i. What information can be shared?

- **e.** Disclosures
  - **i.** What must employees disclose when using social media and what must they not disclose?
- **f.** Legal Issues
  - **i.** What legal restrictions must be applied to social media usage?
- **g.** Level of Engagement
  - **i.** What are the expectations of engaging with the community and what internal and external resources are required?
- **h.** Managing Friends of the Company
  - **i.** Understand the dangers and opportunities posed by Friends and review endorsements, profile information that is linked and shared, and manage trust.
- **i.** How to Handle Negative Comments
- **j.** Press Inquiries
  - **i.** Define responsibilities for dealing with the press.
- **k.** Third-party Employees
  - **i.** Identify process for managing third-party relationships
- **l.** Restrictions on Trademarks and Intellectual Property
  - **i.** How are trademarks, copyrights, and IP managed?

4. IT Security Policies

- **a.** The purpose of these policies is to establish the technical guidelines for IT security and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the company's comprehensive set of security policies. This policy purposely avoids being overly specific in order to provide some latitude in implementation and management strategies.
- **b.** Social Media Sites Authentication
  - **i.** Define complexity of passwords for all in-house hosted application and third-party hosted social media applications.
    1. Password Construction
       The following statements apply to the construction of passwords for network devices: Eight characters, with a mix of letters, numbers, and special characters (such as punctuation marks and symbols).

Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary, should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

2. Change Requirements
   Passwords must be changed according to the company's Password Policy. Identity requirements that apply to changing network device passwords.
3. Password Policy Enforcement
   Where passwords are used an application must be implemented that enforces the company's password policies on construction, changes, reuse, lockout, etc.
4. Administrative Password Guidelines
   As a general rule, administrative access to systems should be limited to only those who have a legitimate business need for this type of access.

c. In-House Deployed Social Media Applications

i. Failed Logons
Repeated logon failures can indicate an attempt to "crack" a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the company must lock a user's account after five unsuccessful logins.

ii. Logging
Logging needs vary depending on the type of network system and the type of data the system holds. The following sections detail the company's requirements for logging and log review.

1. Application Servers
   Logs from application servers are of interest since these servers often allow connections from a large number of internal and/or external sources. At a minimum, logging of errors, faults, and login failures is required.
2. Network Devices
   Logs from network devices protecting the application servers are of interest since these devices control all network traffic, and can have a huge impact on the company's security. At a minimum, logging of errors, faults, and login failures is required.

iii. Log Management

1. Log Review
   Log management applications can assist in highlighting important events, however, a member of the company's IT team should still review the logs as frequently as is reasonable.
2. Log Retention
   Logs should be retained in accordance with the company's Retention Policy.

iv. Intrusion Detection/Intrusion Prevention
The company requires the use of either an IDS or IPS on critical application servers.

v. Security Testing
Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the company's network security.

1. Internal security testing
2. External security testing

vi. Social Media Application Documentation
Documentation, specifically as it relates to security, is important for efficient and successful application management.

vii. Antivirus/Antimalware

viii. All application servers and end-user systems that connect to the application servers should have antivirus/antimalware software running.

ix. Software Use Policy

1. Software applications can create risk in a number of ways and thus certain aspects of software use must be covered by this policy.
2. All downloadable social media end-user software and applications for desktop, laptops, and mobile devices should be approved by IT Management.

x. Suspected Security Incidents

1. When a security incident is suspected that may impact a network device, the IT Staff should refer to the company's Incident Response policy for guidance.

- **d.** Third-party Hosted Applications
  - **i.** Service level agreement
    Review all service level agreements with sites and application providers.
  - **ii.** Updates
    Upgrades must be in place for updates, upgrades, and hotfixes to address security concerns
  - **iii.** Testing
    1. Third-parties must provide proof of security testing of their applications or allow the company to test the application for security weaknesses.
    2. Third-parties must provide proof of security infrastructure and policies that maintain a secure environment for customer data.
- **e.** Education and Training
  - **i.** IT Security is responsible for training end users on security requirements for all hardware and software resources.
  - **ii.** HR is responsible for policy and process training.
  - **iii.** Hold a yearly training program and ongoing updates to alerts users of new risks and security measures.

5. Social Media Do's and Don'ts

- **a.** What are the major Do's and Don'ts?
- **b.** Social Media Do's
  - **i.** Add value, promote the company in a positive light, educate, be a brand ambassador, respond to customers, engage in conversations, be a knowledge resource, build relationships, know the restrictions on content, understand the risks of the mediums, check all facts, provide disclaimers, gain feedback, check regulatory risk, understand legal ramifications, secure communications, secure and protect customer information, understand privacy requirements, etc.
- **c.** Social Media Don'ts
  - **i.** Discuss confidential information, share private customer information, share derogatory comments, access unsecured or unencrypted channels, discuss customer activity, post internal information, associate personal life with corporate accounts, disparage competitors, disparage partners, be condescending or patronizing, etc.

6. Brand Guideline Policy
    a. What is the brand policy and what are the guidelines for discussing and promoting the brand?
7. Twitter Usage Policy
    a. Identify what Twitter should be used for.
    b. Identify objectives (access, brand monitoring, identity management, research, customer communications, media coverage, etc.).
    c. Policy Team Ownership
    d. Identify who can source and publish tweets.
    e. Content Guidelines
        i. Identify content requirements such as frequency, context, content, tone, hashtag usage, followers, following, etc.
        ii. Link shortening policy
    f. Re-tweeting and Following
        i. Focus areas: research, partners, industry news, statistics, other relevant content
        ii. Research, partners, industry news, statistics, other relevant content
    g. Product-specific Accounts Management
        i. Link accounts to products
        ii. Monitor specific accounts
8. Facebook Usage Policy
    a. Identify what Facebook should be used for.
    b. Identify objectives (brand monitoring, marketing, community engagement, partnership development, lead generation, etc.).
    c. Policy Team Ownership
    d. Identify who can use Facebook and post from company accounts.
    e. Content Guidelines
        i. What content is applicable and allowed?
        ii. Content types and sources (such as events, news, surveys, photos, etc.)
        iii. Tone of community engagement and interaction (personal, corporate, friendly, professional)
        iv. Online contest general guidelines from a security perspective

9. Company Blogging Policy
    a. Define the purpose of corporate blogging
    b. Objectives
    c. Policy Team Ownership
    d. Identify who is responsible for blogging
    e. Content Guidelines
        i. Define what content is allowed in blogs
        ii. Identify video policy for blogs
10. Personal Blogging Policy
    a. Identify how employees are allowed to use company information in personal blogs and social network posts, and when and where personal blogs can be accessed.
        i. What are the limitations?
        ii. What corporate IP can be used?
        iii. What can be said about company products and services?
        iv. Identify relevant Human Resources policies that restrict employee dissemination of company information in any form.
        v. What company confidential or other information can be posted?
    b. Approval process
    c. Disclaimer
        i. What disclaimers must employees use?
    d. Disclosure
        i. What must employees disclose and not disclose on their blogs?
    e. Endorsements
11. Employee Code of Conduct Policy
    a. Reference Human Resources handbook on code of conduct.
    b. Do not damage the company reputation.
    c. Use of inappropriate comments.

Wrap Up

Your Social Media Policy is the foundation of your operations and procedures. Constructing it is challenging, as it has to take into account new functions that many companies have not had to deal with before and has to be constantly updated. Also, departments must collaborate in ways they haven't done previously. To develop a comprehensive policy, you have to address all the major aspects of the H.U.M.O.R. Matrix. A key driver is how the different departments work together daily to achieve a baseline level of secure operations.

Improvement Checklist

- ☐ Is there ongoing communications and collaboration across departments?
- ☐ Have you defined specific policies for internally hosted applications versus externally hosted applications?
- ☐ Are you managing the policy on a constant basis?
- ☐ Did you create a new role for the Community Manager?