WHITE PAPER

Why All Organizations Need to Manage and Archive Social Media

An Osterman Research White Paper

Published April 2012

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Social media is among the most pervasive and fastest growing application categories: roughly one in every eight people on earth has an account with Facebook, the most popular social media property. In 2011, 48 hours worth of video were uploaded to YouTube each minute, up from eight hours per minute in 2007[i]. Facebook took 852 days to reach 10 million users, whereas Google+ took only 16 days to hit this user count[ii].

Osterman Research's own statistics indicate that social media is used heavily in the workplace: a survey[iii] conducted during the first quarter of 2012 found that the average employee spends 28 minutes per day using social media during work hours (not counting time spent away from work), or 2.9 workweeks annually. And, while there are many benefits to social media in the workplace, there are also risks, as the same survey found:

- 24% of organizations have had malware infiltrations through Facebook, 7% through Twitter, and 7% through LinkedIn.
- 13% had experienced the leakage of sensitive or confidential information through Facebook, 9% through Twitter and 10% through LinkedIn.
- 73% to 79% of organizations do not archive their users' content posted to these "Big Three" social media properties.
- 13% of organizations have terminated an employee because of something they posted on a social media site.

Despite the problems associated with the use of social media, 81% of organizations allow the use of Facebook, or have a policy limiting or prohibiting its use that goes unenforced. The same applies for 84% of organizations with regard to Twitter – it's 94% for LinkedIn. Moreover, only 19% of organizations have deployed enterprise-grade social media platforms. By "enterprise-grade" social media, we distinguish it from "public" tools like Twitter or Facebook to mean a dedicated social media platform that has been deployed specifically for use by employees, business partners and others.

KEY TAKEAWAYS

While social media can be extremely useful, its use must be managed properly just like any other corporate communications, collaboration, or information-sharing tool. Toward that end, there are five things that organizations must do:

- Create, enforce and update policies focused on appropriate use of social media.
- Archive business records in social media streams that might be required to ensure regulatory or legal compliance.
- Monitor incoming social media content for malware and other threats that could steal corporate data, financial assets or cause other problems.
- Monitor outbound social media data streams to prevent sensitive data or offensive content from being sent from corporate resources.
- Consider implementing an enterprise-grade social media platform in addition to "public" platforms like Facebook and Twitter to help address these other issues.

ABOUT THIS WHITE PAPER

This white paper discusses the various risks that organizations face from unmanaged use of social media. It also offers advice on how organizations can mitigate these risks while at the same time realizing the competitive advantages that the use of

Osterman Research's own statistics indicate that social media is used heavily in the workplace: a survey conducted during the first quarter of 2012 found that the average employee spends 28 minutes per day using social media during work hours.

social media can offer. Finally, it offers a brief overview of Micro Focus, the sponsor of this document, and the company's relevant offerings.

RAPID GROWTH IN THE USE OF SOCIAL MEDIA

GROWING USE OF "PUBLIC" SOCIAL MEDIA

Leading "public" – or non-enterprise – social media platforms are widely used and are growing in popularity as evidenced by published statistics:

- Facebook, the most widely used social media tool, had 166.0 million US visitors in November 2011[iv]. The company reports that it had 845 million monthly active users and 483 million daily active users as of December 2011[v]; iCrossing estimates Facebook will reach one billion active users by August 2012[vi].
- Google Sites, whose traffic was mostly generated by YouTube, had 147.2 million unique US viewers in May 2011 (2.2 billion viewing sessions) who each averaged 311 minutes of viewing[vii].
- LinkedIn had 35.0 million US visitors in November 2011[viii].
- Twitter had 35.4 million US visitors in November 2011[ix], an increase of 8.4 million from May 2011[x]. As of mid-March 2012, Twitter had 526.2 million registered accounts[xi].
- Tumblr had 15.9 million US visitors in November 2011[xii], up 10.7 million from May 2011[xiii].
- Pinterest had nearly five million unique US visitors in November 2011[xiv] and roughly 20 million users in March 2012[xv].

As evidence of the growing importance of social media in the context of just its messaging capabilities, an Ovum study found that text messaging is on the decline as a result of messages sent via social media – down 6% in 2010 and 9% in 2011[xvi]. This by no means implies that use of mobile platforms is waning – in fact, mobile is becoming *more* important – but rather that communication within social media is displacing a growing proportion of traditional modes of communication like text messaging.

Communication within social media is displacing a growing proportion of traditional modes of communication.

GROWING USE OF ENTERPRISE SOCIAL MEDIA

An Osterman Research survey conducted during the first quarter of 2012 found that 19% of the organizations surveyed have deployed an enterprise-grade social media platform. This is significantly below the level of use for consumer-focused tools, such as Facebook (used by 36% of employees on corporate networks), YouTube (30%), LinkedIn (29%) and Twitter (17%).

That said, there are a substantial number of corporate users of enterprise social media platforms, including Jive's 15 million users[xvii], Yammer's four million users as of February 2012 (up from 1.6 million at the end of 2011[xviii]), Socialtext's 6,500+ corporate customers[xix], Salesforce.com Chatter's roughly three million users, and IBM's many millions of Connections users.

WHERE IS ENTERPRISE SOCIAL MEDIA GOING FROM HERE?

Despite the comparatively low use of enterprise-grade social media platforms at present, Osterman Research anticipates significant growth in the market for these tools as a result of two key drivers:

- Decision makers are increasingly realizing the value of social media for collaboration, knowledge sharing, skills discovery and a variety of other purposes; and are considering social media as a means of improving employee

productivity and increasing the speed of decision-making, and thereby delivering a competitive advantage. As evidence, the survey cited above found that while only 14% of organizations have conducted any sort of return-on-investment analysis for social media, another 39% indicated that they need to do so, implying that many decision makers view social media as a business productivity tool.

- Decision makers are beginning to realize the significant level of threats that they face from the unregulated use of non-enterprise tools in a workplace context. As a result, they are deploying capabilities to address specific threats as discussed later in this white paper, and are deploying enterprise-grade social media solutions to address the deficiencies in consumer/free tools.

It is important to understand, however, that consumer/public platforms are not best suited to deal with enterprise social media requirements and the security concerns discussed below.

Managed properly, social media can create a sense of community and affirmation for employees, business partners and others in virtually any organization. It can provide a means of information sharing and gathering that is simply not possible with other corporate tools.

SOCIAL MEDIA AND THE PARADIGM SHIFT IT REPRESENTS

WHY IS SOCIAL MEDIA SO PERVASIVE?

Social media is incredibly pervasive, consuming large amounts of the time that users spend online. For example, in November 2011, the average Facebook user spent 394 minutes on the site[xx], or 13 minutes per day – up 37% from 12 months earlier. Users of Tumblr.com and Pinterest spent 142 and 88 minutes in November 2011 on each site, respectively.

THE USER PERSPECTIVE

A key reason that social media is increasing in popularity, is that it represents a community of like-minded individuals to whom people can turn to both learn and share (or overshare) information. As one marketing consultant noted about Facebook, "It's one of the very few experiences that almost always delivers on expectations. A Facebook session always includes something that each individual cares about. It's much more reliable and friendly than most real friends. Facebook reaffirms connections to clan, tribe, class and community. Facebook might just be the antidote to existential loneliness."[xxi]

Similarly, Twitter is akin to a 24x7 water cooler conversation with hundreds or thousands of people in whose opinion one might be interested. It provides a connection to others for purposes of both sharing and gathering information in a manner and breadth that is simply not possible or practical with other types of tools like email or instant messaging.

THE BUSINESS PERSPECTIVE

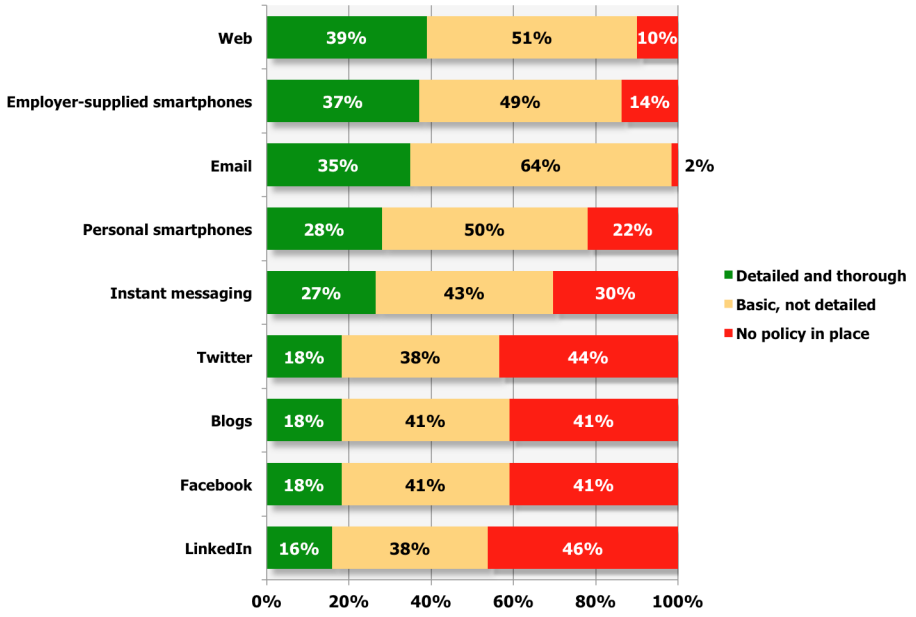
Therein lies one of the fundamental benefits of social media from a business perspective: managed properly, social media can create a sense of community and affirmation for employees, business partners and others in virtually any organization. It can provide a means of information sharing and gathering that is simply not possible with other corporate tools. Moreover, if organizations can create the appropriate environment within their organization, viewing it as an integral component of their larger corporate culture, they can speed decision-making and improve the quality of corporate decisions, they can improve the speed and quality of customer service, and they can improve the ability and desire of employees to collaborate more efficiently and effectively, all resulting in a significant competitive advantage. They can also leverage their employees to serve as an amplification channel for the messages the company desires to promote on a wider scale.

SOCIAL MEDIA AND THE RISK IT REPRESENTS

MOST ORGANIZATIONS DO NOT HAVE ADEQUATE SOCIAL MEDIA POLICIES

The vast majority of organizations do not have detailed and thorough social media policies in place. For example, as shown in the context of other communication and collaboration tools in use in mid-sized and enterprise environments, the "Big Three" social media tools rank well behind other tools in terms of the thoroughness of the policies that have been implemented to protect against misuse, as shown in the following figure from a July 2011 report[xxii] published by Osterman Research.

Thoroughness of Corporate Policies for Various Systems



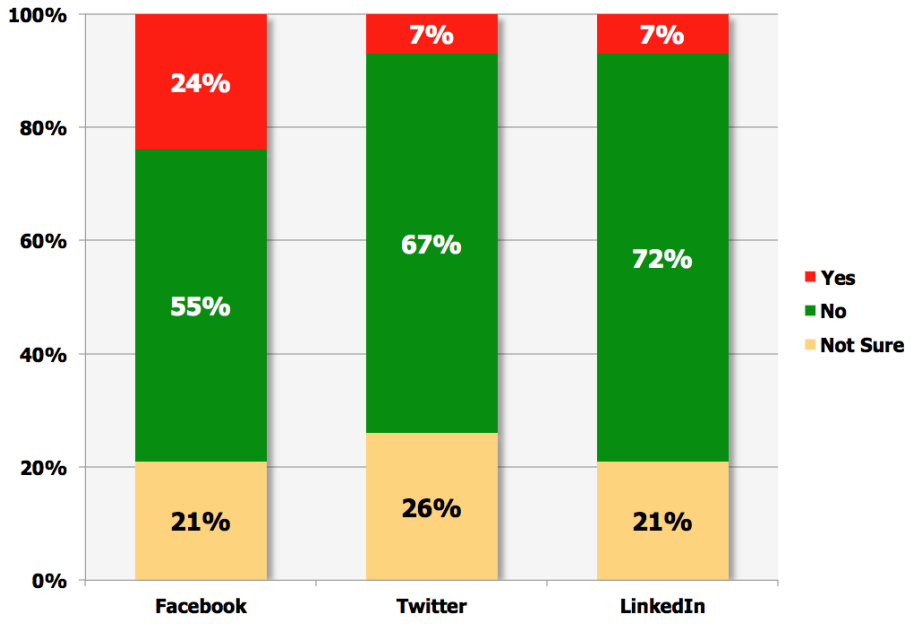
Moreover, even where policies exist, many organizations do not enforce compliance rules in a methodical and meaningful way. For example, Osterman Research found in a survey conducted during the first quarter of 2012 that only 13% to 20% of organizations monitor posts to Facebook, Twitter and LinkedIn, and enforce corporate compliance rules. Further, 76% to 83% of organizations either ask individuals to comply with corporate policies focused on Facebook, Twitter and LinkedIn but do not screen for content, or they do nothing.

THERE IS ENORMOUS POTENTIAL FOR MALWARE INFILTRATION

Among the chief threats that organizations face from unmanaged use of social media is the potential – and reality – of social media used for ingress of malware. As shown in the following figure, Osterman Research has found that malware has infiltrated 24% of organizations through Facebook and 7% of organizations through Twitter and LinkedIn. More troubling, however, is the fact that a large proportion of organizations simply are not sure whether or not malware has entered through these tools.

The vast majority of organizations do not have detailed and thorough social media policies in place. Even where policies exist, many organizations do not enforce compliance rules in a methodical and meaningful way.

Infiltration of Malware Through Various Social Media Tools
"Has malware ever infiltrated your corporate network through the following tools?"



While traditional anti-virus and anti-malware tools can be somewhat effective at blocking these threats, a zero-hour threat detection and remediation capability is essential to block malware that can enter through social media, including those that can enter through mobile device where a substantial proportion of social media use occurs. Among the various types of malware that can be introduced into an organization through the unfettered use of social media:

- **Koobface**
  This worm targets primarily Facebook, but also Twitter, MySpace and other social media sites. Its goal is to gather login information for purposes of building a peer-to-peer botnet.

- **Bugat**
  Related to the infamous keystroke-logging malware Zeus, Bugat has been delivered in a large-scale phishing attack against LinkedIn.

- **Boonana**
  Written in Java and first reported in late October 2010, Boonana targets Macs and operates much like Koobface.

BUSINESS RECORDS IN SOCIAL MEDIA ARE NOT BEING ARCHIVED

Another serious problem with current management of social media is that the vast majority of organizations are not yet archiving their social media content, such as Facebook posts or tweets. This, despite the growing number of regulations, court decisions and other guidance that strongly suggests that social media content should be archived like email or instant messages. For example, among the many regulatory requirements to archive social media content are the following:

- Various rules issued by the Financial Industry Regulatory Authority (FINRA) require supervision of communications by registered financial services representatives. For example, FINRA Regulatory Notice 10-06 states that "Every firm that intends to communicate, or permit its associated persons to communicate, through social media sites must first ensure that it can retain

While traditional anti-virus and anti-malware tools can be somewhat effective at blocking threats, a zero-hour threat detection and remediation capability is essential to block malware that can enter through social media.

records of those communications as required by Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 and NASD Rule 3110." FINRA issued Regulatory Notice 11-39 (*Social Media Websites and the Use of Personal Devices for Business Communications*) in August 2011 that addresses questions raised by firms that are affected by 10-06.

- The Securities and Exchange Commission (SEC) published a National Examination Risk Alert (*Investment Adviser Use of Social Media*) on January 4, 2012 that spells out investment advisers' obligation related to the use of social media. On the same day, the SEC issued sanctions against an individual who, although not a registered broker-dealer, used social media to make offers for the purchase and sale of fraudulent financial products[xxiii].

- According to FRCP rules, all employee-created social media content that is work-related, regardless of whether or not it was created on a personal account, is discoverable. Not only should this be archived and supervised according to corporate policies, but archiving this data in a siloed bin may be required to address employee privacy issues.

- The National Archives and Record Administration (NARA) continues to refine policy regarding the retention of social media communication. An October 2010 NARA bulletin explains that "Open and transparent government increasingly relies on the use of these [Web 2.0] technologies, and as agencies adopt these tools, they must comply with all records management laws, regulations, and policies. The principles for analyzing, scheduling, and managing records are based on content and are independent of the medium; where and how an agency creates, uses, or stores information does not affect how agencies identify Federal records.[xxiv]"

- The US Department of Defense has provided formal guidance on the use of Web 2.0 tools, which includes guidance that "all users of these Internet-based capabilities must be aware of the potential record value of their content, including content that may originate outside the agency."

- The Environmental Protection Agency has published *Interim Guidance for EPA Employees who are Representing EPA Online Using Social Media*, requiring that "agency records created or received using social media tools must be printed to paper and managed according to the applicable records schedule in a recordkeeping system."

- The US State Department's official policy, *Using Social Media*, requires a site sponsor to be the record keeper for content that must be preserved long term, requiring that records "be maintained with related records or managed through an acceptable records management application."

- While the healthcare industry has thus far received relatively guidance specifically on point for social media retention or management, existing regulations would seem to apply to social media. For example, if a physician or other healthcare professional posts content about a patient to a social media site, HIPAA or Federal Substance Abuse Confidentiality laws may apply in the context of receiving and retaining patient approval to post this content[xxv].

Several recent legal cases have also underscored the growing importance of retaining social media content:

- *Smizer v. Cmty. Mennonite Early Learning Ctr.*[xxvi]
  In this case, the defendant claimed that the plaintiff was terminated because of an inappropriate post on Facebook, a claim that the plaintiff denied. The Court agreed with the plaintiff, ordering discovery of other relevant information and not accepting at face value the defendant's claim that the Facebook post was the sole reason for the termination.

According to FRCP rules, all employee-created social media content that is work-related, regardless of whether or not it was created on a personal account, is discoverable.

- *Katiroll Co. v. Kati Roll & Platters, Inc.*[xxvii]
  The plaintiff sent the defendant a notice asking them to take down certain Facebook pages. After the defendant did so, the plaintiff asked the Court for sanctions against the defendant for spoliation because the defendant had not preserved the pages in PDF format. This case is particularly interesting because the Court acknowledged the obligation to preserve content posted to social media Web sites. Specifically, the Court found that "given that Defendants have a discovery obligation to produce them (the Facebook pages) and that only Defendants knew when the website would be changed, it is more appropriate for Defendants to have that burden."

- *Lester v. Allied Concrete Co.*[xxviii]
  The Court fined an attorney $522,000 for telling his client to delete various images from his Facebook and Myspace profiles. The client was fined $180,000 for following the advice to destroy evidence.

Underscoring the growing importance of social media in legal cases is one study that found 674 federal and state court decisions that involved social media evidence for the 22-month period ended November 1, 2011[xxix].

Underscoring the growing importance of social media in legal cases is one study that found 674 federal and state court decisions that involved social media evidence for the 22-month period ended November 1, 2011.

SOME EMPLOYEES MISUSE SOCIAL MEDIA

Another serious threat that organizations face is the misuse of social media by employees. For example:

- In 2009, an employee of Ketchum, a public relations firm, used Twitter to post insulting comments about the city of Memphis shortly before presenting to the worldwide communications group at FedEx – Memphis' largest employer. An employee of FedEx discovered the tweet, responded to the tweeter, and then copied FedEx's senior managers, the management of FedEx's communication department and the management of Ketchum[xxx].

- Employees at the Tri-City Medical Center in Oceanside, California posted patient information on Facebook[xxxi].

- The president of The Redner Group, the (now former) public relations firm for 2K Games' Duke Nukem Forever tweeted in June 2011 "Too many went too far with their reviews … we are reviewing who gets games next time and who doesn't based on today's venom," publicly threatening to blacklist those who negatively reviewed the game[xxxii].

- In 2009, authorities investigated a situation in which election exit poll results for three German states were leaked on Twitter prior to the polls closing[xxxiii].

- A hospital employee in Hawaii with access to patients' medical records illegally accessed another person's records and posted on MySpace that the individual had HIV[xxxiv].

A West Allis, Wisconsin employee was fired for a post she made on her Facebook page claiming that she was addicted to alcohol and various prescription and illegal drugs, although the employee claimed that her comments were made in jest[xxxv].

HOW SHOULD SOCIAL MEDIA BE MANAGED?

Osterman Research believes that there are five important issues that decision makers must consider in the context of their social media management:

1. DETERMINE BENEFITS AND HOW BEST TO MANAGE RISKS

An organization should determine if it can obtain competitive advantage through the use of social media – whether consumer/public or enterprise-grade – instead

of making a knee-jerk decision not to use these tools because of security or other risks they might pose.

To evaluate this question, an organization's various business units and its IT department should conduct a complete evaluation of how social media is used by various functions across the enterprise, which tools are used and why they are used. This audit should also include an analysis of how these tools might be used in the future, how competing firms are using them, and any new capabilities that might be required in the future.

Such an evaluation could reveal that there is a major disconnect between what IT, security or compliance perceives as a legitimate application of social media and what individual users or business units perceive to be legitimate. The goal is to balance the interests of both groups and derive the greatest benefit from the use of social media while still remaining compliant with corporate policies and security requirements. For example, specific applications of social media discovered in this analysis might include:

- Marketing, communications, PR teams and spokespeople who want the ability to post commentary, create events and use the full functionality of social media.
- Corporate users, such as Human Resources and legal staff who need to research new hires and investigate shared content.
- Regulatory compliance teams who must not only maintain records of shared content and activities, but also approve and moderate subject matter.
- Employees who utilize social media to prospect for business, network with customers and partners and collaborate with suppliers.
- The analysis might also reveal the need for an enterprise-grade social media capability to enhance employee productivity, improve customer support, or improve decision making by increasing the velocity and availability of information throughout the company.

2. DEVELOP, ENFORCE AND UPDATE SOCIAL MEDIA POLICIES

The next step is to implement policies that will focus on creating an appropriate balance between employee freedom to gather information and communicate via social media, the business benefits that will be derived from the use of these tools, compliance with industry regulations, and advice from legal counsel. A social media policy should be considered regardless of whether the company chooses to use consumer/public tools or if it determines that an enterprise networking solution is best. Considerations for these policies should include:

- **Adding social media as part of the overall policy set**
  Policies focused on the use of social media tools should be a key part of an overall messaging and communication policy that focuses on the use of corporate email, personal Webmail, instant messaging tools, collaborative workspaces, cloud-based storage tools and any other capability through which individuals might share corporate information.
- **Policy granularity**
  Sufficient granularity should be provided in these policies so that differing roles within the organization are clearly subject to different policies. For example, energy and securities traders may be subject to different rules about their use of social media than clerical staff, senior managers should be subject to different policies when communicating with external auditors than when they communicate with employees, formal communications that

Implement policies that will focus on creating an appropriate balance between employee freedom to gather information and communicate via social media, the business benefits that will be derived from the use of these tools, compliance with industry regulations, and advice from legal counsel.

represent a company position should be subject to different scrutiny than personal communications, and so on.

- **Acceptable use**
  Corporate social media policies should include a detailed discussion about appropriate use of social media tools, including requirements not to post sexually or racially offensive comments or images, not to include links to inappropriate Web sites, not to defame or slander others, not to post content that could run afoul of copyright laws, not to post personnel records or other sensitive information, to ensure that posts are in good taste, and the like.

- **Identifying specific tools that can and cannot be used**
  Specific tools that can and cannot be used should be specified clearly, preferably along with a rationale for the decision. This includes the social media sites themselves, as well as the platforms on which these sites are accessed – home computers, smartphones, desktop computers at work, etc. While some decision makers may opt for a draconian approach and create policies that prohibit the use of Facebook, Twitter, LinkedIn or other tools on corporate platforms, such an approach will be unlikely to work and will simply prompt employees to use their personal devices to access these tools. Instead, a more reasonable approach of allowing appropriate use of these tools will better serve management and employees.

- **The right to monitor**
  Corporate policies should clearly state that management reserves the right to monitor employee communication via social media, when it has the right to act on this information, and that content may be retained for an indefinite period.

- **Succession planning**
  Some discussion of succession planning should also be a part of social media policies. For example, when an employee leaves the organization, the corporate policy should include provisions about "ownership" of the followers or friends of that employee. For example, do followers on Twitter belong to the employer or employee? Are an employee's Facebook posts the property of his or her employer if they were posted during work hours?

- **Data breaches**
  Social media policies should also spell out the corporate reaction to a data breach and the consequences of a policy violation. For example, if an employee mistakenly tweets a product announcement a day before the press release is issued, or mistakenly posts trade secrets on a Facebook page, what are the consequences?

3. MANAGE SOCIAL MEDIA APPROPRIATELY

For any type of social media tool, every organization should deploy technologies that will do various things:

- **Monitor posts, tweets and other outbound content**
  Employee posts on every social media protocol that might be used should be monitored for content that violates corporate, regulatory or legal policies – particularly in heavily regulated industries. This monitoring may be after the fact, such as sampling employee posts to check for inappropriate content; or it might be in real-time to monitor posts before they leave the organization.

- **Scan for and remediate malware**
  It is also important to block threats that can enter an organization through social media. This is particularly important given a) the widespread use of shortened URLs that offer the user no visual cues about the veracity of the link, and b) the fact that many social media tools can display content

Corporate policies should clearly state that management reserves the right to monitor employee communication via social media, when it has the right to act on this information, and that content may be retained for an indefinite period.

provided by individuals to whom users have not given permission to display posts.

One of the fundamental problems with social media from a security perspective is that these tools are generally less well defended than more established tools like email. Given the rapid increase in the use of many of these tools, many IT departments are scrambling to keep up with the rapid growth of social media tools, leaving organizations vulnerable to malware infiltration. As noted earlier, nearly one in four organizations has been the victim of Facebook-related malware. In fact, a recent Osterman Research survey found that in addition to Facebook, organizations have had malware infiltrate through a variety of social media tools, including YouTube and Google+.

Using an enterprise-grade social media platform will alleviate many of these concerns.

- **Archive business records in social media**
  It is critical to archive and log all content that might constitute a business record and that might need to be retained for long periods. It is normally easier to archive or log all social media content than take the risk that some important content might slip through and not be retained, but this will depend to a large extent on the industry in which an organization operates, management's tolerance for risk, advice of legal counsel and other factors. An important part of content logging is to ensure that the identity of the individuals who use social media tools is clear and that content can be tied back to their corporate identity.

  An important best practice is to integrate social media archiving with email and other content archiving. This ensures that legal holds, as well as searching for content during early case assessment and e-discovery, are much easier, less time-consuming and less prone to missing important content. Many enterprise platforms will be able to handle the archival requirements of an enterprise. Shifting conversations from public open forums to an internal social intranet will also ensure that risky conversations take place behind the firewall rather than in the public eye.

One of the fundamental problems with social media from a security perspective is that these tools are generally less well defended than more established tools like email.

4. CONSIDER ANALYTICS

One of the more important benefits of social media is that it provides a wealth of information that can be used to help organizations understand their markets and to improve decision-making. For example, by mining data from tweets and Facebook posts and performing both text and sentiment analysis on this unstructured data, decision makers can gain insight into how their customers and prospects are reacting to changes in a product, advertising campaign, price change or any number of other issues. The value of analytics when applied to social media data is that – unlike traditional market or marketing research – social media analytics provides the ability to monitor and analyze a market in near real-time. Analytics will become increasingly important with the growth of social media because it allows rapid and granular decision-making.

5. CONSIDER DEPLOYING ENTERPRISE SOCIAL MEDIA

All organizations should consider deploying enterprise-grade social media platforms. One of the fundamental benefits of leading enterprise tools is that they are purpose-built to protect against the key issues outlined above that organizations face from unmanaged use of social media – namely, security, archiving of content, permissions controls and compliance. Because enterprise-grade platforms do not have their origin in the consumer/free space where these types of controls are a lower priority, enterprise tools are built from the ground up to provide robust protection and management tools. This ensures that

organizations can minimize the risks they face when using only consumer/free tools.

That said, it is important to note that we are not advocating an either-or decision on the use of enterprise-grade social media tools or those that are aimed at the consumer/free market. Moreover, enterprise-grade social media is not a panacea for every type of threat, such as malware delivered via mobile devices. Osterman Research firmly believes that organizations should deploy both types of capabilities:

- Enterprise-grade social media tools are designed primarily to improve collaboration within an organization; to improve the quality and speed of decision-making; to create content like wikis, blogs and collaborative documents; to enable improved access to the skill sets of employees across an organization; to integrate social content with CRM tools; to improve the flow, quality and timeliness of information between employees and business partners; and to mitigate the disadvantage of distance for employees who work in geographically separate locations.

- Consumer/free tools like Facebook or Twitter, on the other hand, are more useful for broadcasting content to external parties like customers, prospects and others; for marketing brands and establishing industry leadership; and for understanding the dynamics of a market through analysis of social media information flows. However, these tools require appropriate security, archiving and other management capabilities to ensure that their use provides the same level of protection as those built into enterprise-grade systems.

It is also important to note that there is some convergence occurring between these capabilities, such as enterprise-grade platforms integrating Twitter and other social media feeds.

SPONSOR OF THIS WHITE PAPER

Micro Focus is a global software company with 40 years of experience in delivering and supporting enterprise software solutions that help customers innovate faster with lower risk. By applying proven expertise in software and security, we enable customers to utilize new technology solutions while maximizing the value of their investments in critical IT infrastructure and business applications. As a result, they can build, operate, and secure the IT systems that bring together existing business logic and applications with emerging technologies—in essence, bridging the old and the new—to meet their increasingly complex business demands.

www.microfocus.com
twitter.com/MicroFocus

+1 866 464 9282
+1 646 304 6250