WHITE PAPER

Best Practices for Social Media Archiving and Security

An Osterman Research White Paper

Published August 2016

proofpoint™

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Social media is pervasive in the workplace, not only by employees for their personal use, but also for business purposes. For example, 73% of the organizations surveyed for this white paper employ Facebook for business reasons, 64% use LinkedIn, and 56% use Twitter, in addition to a variety of other social media platforms. Moreover, a large and growing proportion of organizations use enterprise social media platforms, including Microsoft SharePoint, various Cisco social media tools, Microsoft Yammer, Salesforce Chatter and IBM Connections, among many others.

The use of social media provides a number of important benefits that help organizations to become more efficient, that help users speed the decision-making process, and that allow information sharing in a way that is not possible or practical otherwise. However, increasing use of social media – whether consumer-focused or enterprise-grade – comes with several risks and costs:

- The increased likelihood that malicious content can enter an organization through a social media channel. Our research found that 18% of organizations have experienced malware infiltration through social media, although a substantially larger proportion don't know how malware entered.

- The greater likelihood of breaching sensitive or confidential data, either through inadvertent actions on the part of employees, unmanaged sharing of geolocation data, or malicious employee activities.

- The inability to retain the relevant business records and other information that organizations are obliged to preserve. Our research found that 43% of organizations that have deployed an enterprise social platform do not archive information from it and 26% have had to produce content for eDiscovery from the platform.

KEY TAKEAWAYS

To address these issues and mitigate the risks associated with the use of social media, all organizations that employ social media solutions should implement a variety of best practices:

- Conduct an internal audit of social media use to determine which tools are being used, why they are in use, and the business value that organizations are deriving or potentially can derive from them.

- Implement appropriate policies that will address employees' acceptable use of social media tools, identify which roles in the organization should have rights to specific social media features and functions, and clearly spell out the rights of the organization to monitor, manage and archive social media use and content.

- Ensure that employees are trained on corporate social media policies and that they are kept up-to-date on policy changes.

- Deploy the appropriate technologies that will mitigate risks from malware and other threats delivered through social media and corporate social networks.

- Deploy solutions that will archive business records and other content contained in social media and corporate social networks.

- Implement an enterprise social media solution that will not only mitigate the risks associated with use of consumer-focused social media tools, but that will also provide enhanced communication, collaboration and information-sharing capabilities.

ABOUT THIS WHITE PAPER

This white paper presents the results of an in-depth primary research survey conducted with individuals in mid-sized and large organizations who are decision makers or influencers about their organizations' enterprise social strategy. The white paper was sponsored by Proofpoint – information about the company and its relevant offerings is included at the end of this paper.

SOCIAL MEDIA USE CONTINUES TO GROW

CONSUMER-FOCUSED SOCIAL MEDIA

Social media platforms focused on primarily consumer markets are used by hundreds of millions of users worldwide, led by Facebook, which had 1.37 billion active users in 2015. The top 10 social media properties for 2015 (three of which are owned by Facebook) were[i]:

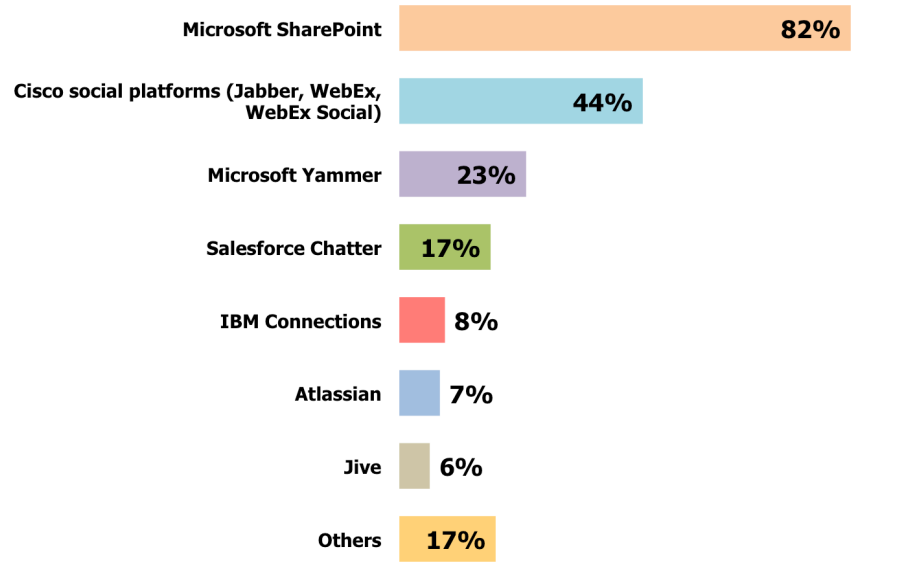
- Facebook: 1.366 billion users
- QQ: 829 million
- QZone: 629 million
- WhatsApp: 600 million
- Facebook Messenger: 500 million
- WeChat: 468 million
- Google+: 343 million
- Skype: 300 million
- Instagram: 300 million
- Twitter: 284 million

A recent Osterman Research survey of end users[ii] found that the typical user employs Facebook, Twitter and LinkedIn a combined total of 13 minutes per workday for work-related purposes, or about 2.7% of a typical eight-hour day. This does not include the substantial use of social media tools for personal applications.

USE OF ENTERPRISE-GRADE SOCIAL MEDIA

Use of enterprise-grade social media platforms is also on the increase, led by Microsoft SharePoint, various Cisco platforms, Microsoft Yammer and Salesforce Chatter, as shown in Figure 1. Please note that we have included SharePoint because of its social media capabilities, although most organizations do not use the platform primarily for enterprise social media purposes.

Figure 1
Penetration of Enterprise Social Platforms
% of Organizations in Which Platform is Deployed



Source: Osterman Research, Inc.

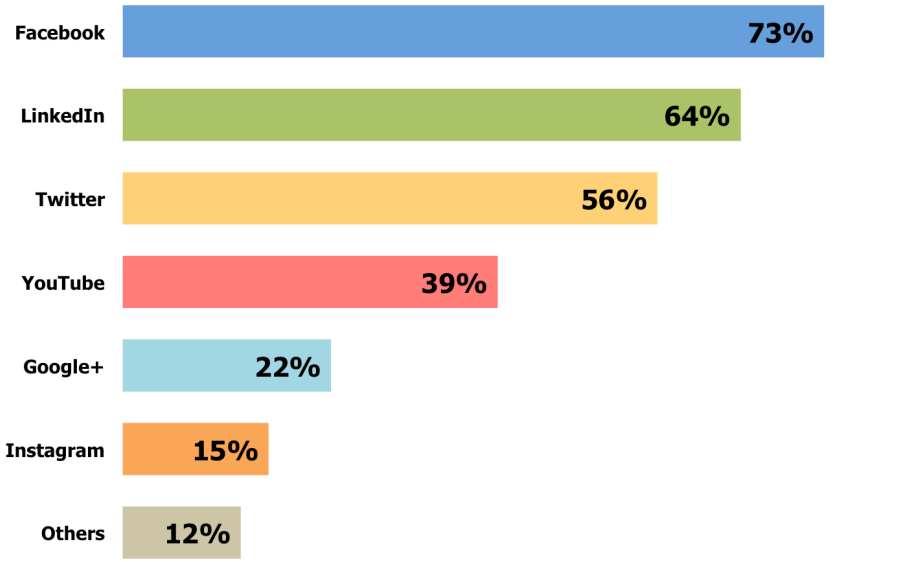
THE GROWING IMPORTANCE OF SOCIAL MEDIA

PENETRATION FROM TWO PERSPECTIVES

There are a number of drivers for the use of consumer-focused social media for work-related purposes, although these drivers vary widely based on the social media platform, the industry in which the organization operates, the extent to which senior managers recognize the value of social media, the overall risk tolerance of the organization, and other factors.

Most use of consumer-focused social media for work purposes is concentrated in the "Big Three" – Facebook, LinkedIn and Twitter – as shown in Figure 2, although a wide range of other social platforms is used and growing in popularity. Moreover, there are 1,000+ social media solutions used worldwide.

Figure 2
Penetration of Consumer-Focused Social Media Platforms for Business
% of Organizations in Which Platform is Deployed



Source: Osterman Research, Inc.

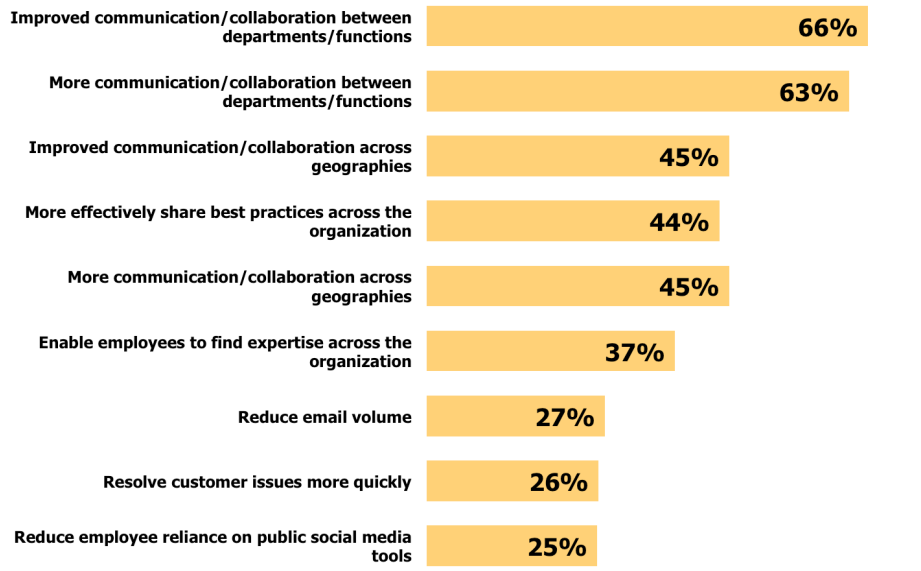
WHAT PROBLEMS DOES SOCIAL MEDIA ADDRESS?

Social media has entered into the workplace in two primary ways:

- Consumer-focused social media has been a mostly employee-driven capability, used initially for personal applications, and later adapted by these employees for specialized job functions like responding to customers and prospects, sharing corporate information, or dealing with complaints. Consumer social media is useful across a wide range of activities, but the primary use cases involve addressing customer service, marketing and related types of issues.

- For enterprise social media, however, the drivers are much more formal, more carefully considered, initiated by IT, and generally focused around issues of improving the quality, agility and the volume of communications, as shown in Figure 3. Interestingly, despite the fact that many discuss social networks as a means of replacing email, this is a much less important driver than many others.

Figure 3
Problems That Organizations Hope to Solve with Enterprise Social Media
% Responding a Consideration or Major Consideration



Source: Osterman Research, Inc.

BENEFITS OF SOCIAL MEDIA

Social media, and enterprise social media in particular, can provide a wide range of benefits, including:

- Faster decision-making capabilities by replacing email as the primary means of collaboration. The ability to share documents, have real-time conversations, and maintain better control over document versions are key benefits of social networks relative to email.
- Customer service can be significantly improved by allowing faster response to customer complaints before they have an opportunity to spread virally.
- Social media provides another avenue for employee-to-employee and employee-to-partner collaboration that offers more real-time capabilities than is possible in email.
- Corporate culture can benefit from improved social media interaction by enabling the development of connections to others in a way that email, corporate directories and more traditional modes of communication and information delivery cannot support.
- Social media can also help users to share the vast pool of knowledge that today resides only in their brains (or on local hard storage). This information might include data as diverse as expertise in particular technologies, past contacts from previous employment, and information about sales prospects that has not been entered into a CRM system.

THE FUTURE OF SOCIAL MEDIA

Osterman Research anticipates two key trends in the development of the social media market over the next several years:

- The use of consumer-focused social media will continue to grow at a healthy pace within the workplace and for personal use. For example, Facebook user

growth has been on a steady upward track over the past few years: total daily active users have increased from 665 million during Q1/2013 to 1.01 billion in Q3/2015, while mobile-only monthly active users have increased from 189 million to 581 million during the same period[iii].

- Enterprise social media use will increase significantly, but largely in the context of email. For example, IBM employs social capabilities within the context of Verse, its cloud-based email platform. We anticipate that Microsoft and other email system providers will increasingly integrate Yammer into the Outlook experience. We found that the messaging system in use within the organizations surveyed had an important or very important influence on the decision about which enterprise social platform to deploy in 52% of organizations. Other solutions, such as the CRM, ERP or enterprise content management solutions in place had much less influence.

What these trends will mean for organizations that increasingly employ social media is that their exposure to various malware and related threats will increase, as will their obligation to retain records generated by and stored in social media systems.

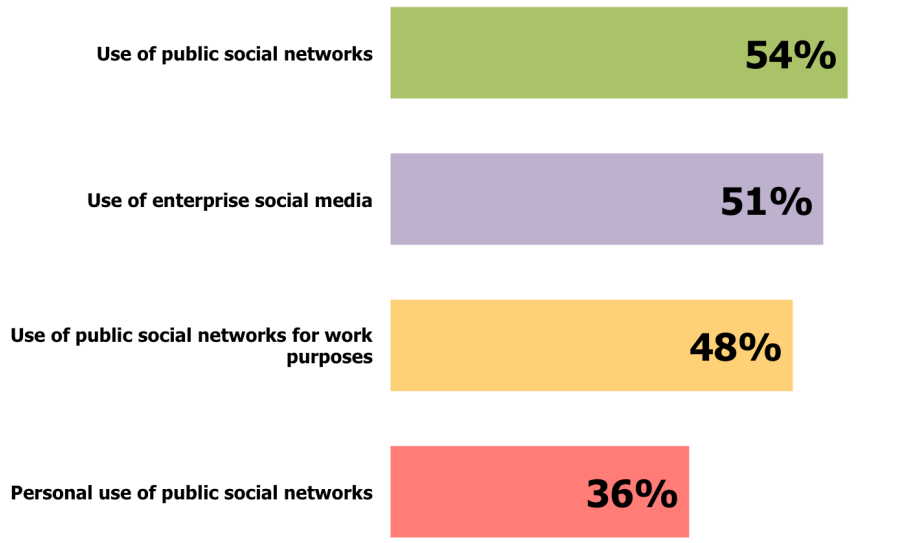
SOCIAL MEDIA IS A MAJOR THREAT

Social media provides a number of benefits, but creates the opportunity for organizations to be exposed to a variety of cyber threats, as well as, legal, regulatory and other problems.

ABSENCE OF SOCIAL MEDIA POLICIES IN MANY ORGANIZATIONS

A large proportion of organizations do not have written policies about the use of various types of social media. For example, as shown in Figure 4, among organizations that have deployed enterprise social media, only 51% have written policies about its use and only 48% of these organizations have a policy about the use of public social networks when employed for work-related purposes.

Figure 4
Presence of a Written Policy About Various Types of Social Media
Among Organizations That Have Deployed Enterprise Social Media



Source: Osterman Research, Inc.

Osterman Research believes that all organizations should have a set of detailed and thorough social media policies that includes a number of things, including:

- Specification about the tools that are and are not permitted for use on the corporate network.
- Rules about whether or not employees can speak on behalf of the company and the extent to which they can do so.
- The types of content that can be shared via social media.
- To what extent personal accounts can be used for business purposes.
- Unambiguous details about who owns social media contacts, such as Twitter followers, if and when an employee leaves the company.
- Initial training of end users on these policies and continual training as policies are updated.

One danger that can occur in the absence of detailed and thorough social media policies is that data can accidentally be leaked through social media channels, resulting in a number of negative consequences. While a leak of information, such as sharing an embargoed announcement, can occur through social media, there are more subtle forms of leakage. For example, an employee who innocently tweets their travel plans might be divulging her company's plan to enter a partnership with another company or to be acquired. Similarly, an employee who shares racially or sexually offensive jokes through social media can create problems with fellow employees, customers, business partners and others. To prevent these types of problems, social media policies should be very clear and prescriptive about employee obligations not to share any information that could harm other employees or the business itself.

CONTENT IS NOT PROPERLY ARCHIVED

Social media platforms – whether enterprise social solutions that have been deployed by an organization or consumer-focused, public systems – contain various types of business records that must be retained. However, our survey found that 66% of the organizations surveyed are not archiving content from external social networks, while 43% of organizations that have deployed an enterprise social platform are not doing so either. Many decision makers are simply not aware of their organizations' legal or regulatory obligations to retain social media content, but this can result in serious problems. While the focus of social media management and control is today skewed heavily toward financial services, there is growing expansion into other heavily regulated industries, as well.

Organizations that do not archive content from social media platforms face significant and growing risks from their inaction. For example:

- Our research found that 26% of organizations have had to produce content for eDiscovery from their enterprise social media platform. Osterman Research anticipates that this figure will grow dramatically over the next two years.
- There are a variety of regulatory obligations to retain business records generated by or stored in social media platforms. For example the Financial Industry Regulatory Authority (FINRA) Regulatory Notice 10-06, Regulatory Notice 11-39, and Rule 2210(c)(6); the Federal Financial Institutions Examination Council (FFIEC) Social Media Guidance; and the Financial Conduct Authority (FCA) GC14/6 all place requirements on regulated organizations to retain relevant social media content.

  A failure to comply with these obligations can be expensive and embarrassing.

For example, a broker who defended a drug company's stock in a Facebook post was fined and temporarily suspended for the post[iv].

- Governments at various levels have open-records requirements and Freedom of Information Act (FOIA) obligations to retain and produce electronic records, which increasingly will include social media posts.

In addition to regulatory obligations to retain social media content, there is a growing body of court decisions that increasingly cite and/or require retention of social media content. Gibson Dunn, in its *2015 Mid-Year E-Discovery Update*[v], reported that "….the number of cases focusing on the discovery of social media continued to skyrocket in the first half of 2015." For example:

- In *D.O.H. v. Lake Central School Corp.*, the plaintiff had deleted relevant information from his Facebook account and the court found that such deletion constituted spoliation of evidence.

- In *Hannah v. Northeastern State University*, two professors posted racist comments on Facebook about a department chair that was denied tenure. The chair sued the university, claiming a hostile work environment. The court found there to be a causal connection between the tenure issue and the plaintiff's complaints about race discrimination.

- In *Calvert v. Red Robin International, Inc.*[vi], the plaintiff was ordered by the court to "bring all materials, electronic or otherwise, including e-mails, Facebook messages, and any other communications he has had with putative class members in this action".

- In *Crowe v. Marquette Transportation*, a US federal court ordered an employee to reactivate his Facebook account, produce a complete copy of his entire Facebook page, and allow his employer to review all of his Facebook messages.

In short, decision makers must realize that social media content is fundamentally no different than more traditional forms of electronic information, and so records contained within social media platforms – whether enterprise or consumer-focused – must be retained and producible for purposes of eDiscovery, litigation holds, regulatory compliance, or corporate best practice. Moreover, it is essential that employers monitor social media posts for egregious violations of corporate policy, the law and regulatory requirements.

DATA CAN BE BREACHED

Social media provides another avenue by which corporate data can be breached. For example:

- **Loss of customer lists**
  In *Eagle v. Morgan*, the court ruled that a LinkedIn profile, including all of its contacts, belongs to the employee if the employer has not established a social media policy specifically stating otherwise. This can result in a company's loss of key business and other contacts to a competitor if an employee leaves. In a similar case, *PhoneDog v. Kravitz*, an employer lost control of a corporate Twitter account and its approximately 17,000 followers after an employee left the company.

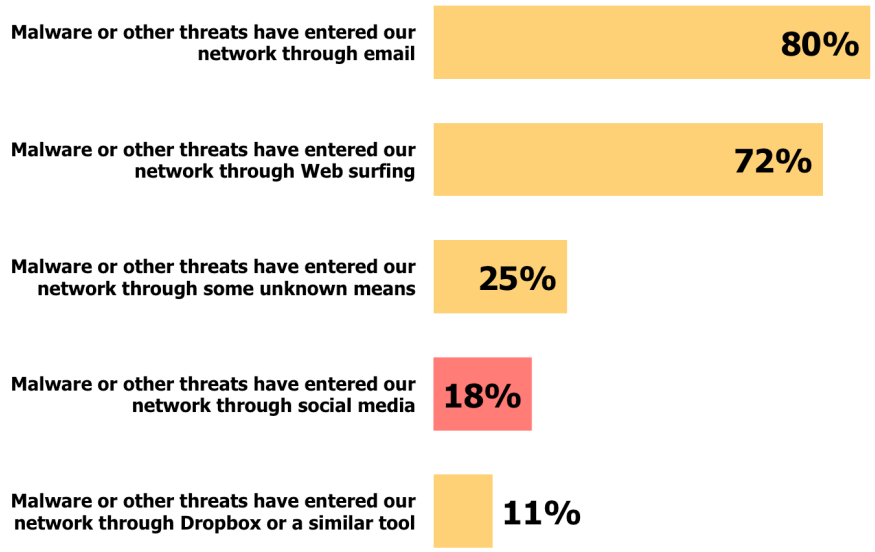
- **Revelation of trade secrets through geolocation**
  Many social media platforms will allow users to indicate their location at the time of a post or will automatically do this for them. Use of geolocation by traveling employees or senior executives can inadvertently reveal confidential information about a merger, acquisition or some other arrangement. This is particularly true when location information makes it easy to infer the company one is visiting, such as Bentonville, AR (Walmart); Corning, NY (Corning, Inc.); Harrison, NY (Pepsico and MasterCard); or Deerfield, IL (Walgreens).

- **Accidental release of confidential information**
  In May 2012, Microsoft accidentally posted information about the availability of the Windows 8 Release Preview on a blog[vii], which followed the accidental release of information about its social search network, which at the time was a confidential research project[viii]. In late 2014, the CFO of Twitter mistakenly sent a message about acquiring another company to his 9,000 followers – he had meant to send it as a direct message to one individual[ix]. In 2011, an HP vice president mistakenly revealed details about the company's cloud-computing offerings via LinkedIn [x].

AN INGRESS POINT FOR MALWARE

The majority of social media users have not had their accounts hacked or been the victim of malware infiltration, but this has occurred for nearly one in five organizations surveyed, as shown in Figure 5. Another one in four organizations cannot determine with any certainty the source of their malware infiltration.

Figure 5
Sources of Malware Infiltration



Source: Osterman Research, Inc.

Social media presents a serious risk of malware infiltration and other threats in a variety of ways. For example:

- Social media platforms like Twitter that limit the number of characters necessitate the use of shortened URLs that can make it much easier for cyber criminals to disguise a link to a malicious site.

- Cybercriminals will often create bogus pages, such as a Facebook page, that will trick victims into downloading malware. Users are sometimes offered a desired capability, such as the ability to find out who visited their Facebook profile, and are willing to provide their login credentials or click on a link to obtain these "features".

- Social media can also be the target of state-sponsored attacks. For example, in December 2015 Twitter issued a security alert to some of its users that they might have been "targeted by state-sponsored actors", the first alert of its type made by the company[xi].

- Moreover, malvertising is on the increase and can infect leading social media properties. A promoted Twittercard was recently discovered that can lead to installation of malware designed to steal Facebook credentials[xii].

Compounding the problem is that many organizations have not deployed solutions specifically designed to monitor or defend against malware infiltration via social media: the survey conducted for this white paper found that 27% of organizations do not monitor social media or social network usage, and 28% have not deployed separate security solutions for social media.

RECOMMENDED BEST PRACTICES

KNOW WHY AND HOW SOCIAL MEDIA IS USED

The initial step for decision makers should be to understand how social media platforms are used in their organization, since this will determine the types and level of effort, policy management and technology solutions required to manage them. For example, decision makers should ask themselves the following questions:

- Is social media being used for informal, non-business-related communications among employees using their personal social media accounts on employee-owned devices?
- Are employees using social media to communicate with prospects, clients or business partners? If so, are they doing so on organization-owned accounts or their own?
- To what extent is social media of any kind used on organization-owned devices?
- Are personally managed social media platforms used to transmit business information?
- Are customer service or marketing teams using social media to communicate "official" corporate messages, such as offers or announcements or responses to customer complaints?
- Are there specific regulations or laws that impact the use of social media or that govern retention of social media content?
- Is the organization monitoring social media conversations?

Getting good answers to these questions is vital in order to determine how to create policies and to decide what security, archiving and other technologies to implement. For example, if social media is used only by employees for informal and/or personal, non-business communications using their personally owned devices and via their own accounts, archiving of this content is normally not necessary or even possible. However, if the customer service, marketing or other groups are sending corporate messages on company-supplied platforms, it is essential that monitoring and archiving technologies be in place to ensure that all relevant content is appropriately reviewed and retained. The same applies to sales conversations that take place with customers and prospects using personal accounts.

IMPLEMENT APPROPRIATE POLICIES

Next, and before any technology decisions are made, decision makers must implement policies that will focus on developing an appropriate balance between the business benefits that will be realized from the use of social media tools, employee freedom to gather information and communicate via social media, the organization's compliance obligations, and advice from legal counsel.

All organizations should consider developing a social media policy regardless of whether or not the company chooses to use consumer-focused social media platforms, or an enterprise social media solution. We recommend that social media policies include the following:

- **Define what constitutes acceptable use of social media**
  Social media policies should include a discussion about the appropriate use of social media tools, including requirements that prohibit posting of sexually or racially offensive comments or images, links to gambling or other inappropriate Web sites, defaming competitors, slandering individuals, content that might violate copyright laws, sharing of sensitive or confidential information, and posts in bad taste, among other things.

- **Integration with other acceptable use policies**
  Social media policies should be a key element of an overall set of communication policies that focus on the use of corporate email, personal Webmail, instant messaging tools, collaboration tools, cloud-based storage repositories and any other capability through which individuals might share corporate information.

- **Include sufficient granularity**
  Social media policies should accommodate differences in employee roles so that different roles can be subject to different policies. For example, senior managers should be subject to different policies when communicating with external auditors vs. communicating with employees. Securities traders should be subject to different social media use rules than their firm's clerical staff. Moreover, formal communications that state a company position should be subject to different monitoring and review practices than employees' personal communications.

- **Identify the platforms that can and cannot be used**
  The policy should clearly identify the social media platform(s) that may and may not be used for business and personal purposes, ideally with a rationale for which platforms are approved and disapproved. This includes the social media sites or tools themselves, as well as the devices on which these sites are accessed – smartphones, home computers, desktop computers at work, etc. While some may opt for a draconian approach and create policies that prohibit the use of any social media tools on corporate devices or networks, this approach will be ineffective and will simply motivate employees to use their personal devices to access these tools while at work. Instead, we recommend allowing appropriate use of social media tools that will serve employees and the organization. However, if employees are using their personal devices and social media accounts for non-business use, there is little that an employer can do to monitor or capture this content anyway, albeit with some exceptions. There needs to be a process in place for vetting, evaluating and approving new social channels that employees would like to use.

- **Clearly state the company's right to monitor social media communications**
  Social media policies should clearly state that management reserves the right to monitor all employee communications when using company-owned resources. This includes personal accounts that have been approved for business purposes, which should have a reasonable expectation of retention/monitoring in accordance with information governance/compliance policy. The policy should also identify the circumstances in which management has the right to act on this information, such as blocking or deleting offensive content. Employees should also be aware that content may be retained for an indefinite period and may be turned over to third parties during eDiscovery, regulatory audits and the like.

- **Provide a means of succession planning**
  Any social media policy should include succession: namely, who owns social media accounts, contacts within them, and the information they contain. For

example, when an employee leaves, the corporate policy should include provisions about who "owns" his or her followers or friends. Do followers on Twitter belong to the employer or employee, regardless of who created the account? Are an employee's corporate Facebook posts the property of his or her employer if they were posted during work hours?

There have been a number of cases in which employees/ex-employees have been involved in legal battles with companies over this issue, including *Eagle v. Edcomm* in the United States and *Whitmar Publications Limited v Gamage and others* in the United Kingdom.

- **Determine how data breaches will be handled**
  Social media policies must also define the appropriate corporate reaction to a data breach and what happens after a policy violation. For example, if an employee mistakenly tweets an announcement before a press release is issued, or mistakenly posts trade secrets on a Facebook page, the consequences of these actions should be clearly spelled out just like they would be for any other type of data breach.

These policies should be implemented in such a way as to achieve employee buy-in, since unreasonable policies simply will be ignored. Moreover, decision makers must periodically revisit and update these policies in order to keep them up-to-date with new social media tools, laws, advice from legal counsel, and best practices.

MONITOR SOCIAL MEDIA USE

Every organization should deploy technologies that monitor social media posts and protect against malware so that decision makers can be proactive rather than merely addressing problems after they occur:

- **Scan for malware**
  It is essential to block threats that can enter an organization through social media, such as malicious advertisements in Facebook or links in Twitter. This is particularly important given the widespread use of shortened URLs that offer the user no visual cues about the veracity of the link, and the fact that many social media tools can display content provided by applications and individuals to whom users have not given permission to display posts.

  One of the fundamental problems with social media is that most platforms are typically less secure than more established tools like email. Many IT departments are not keeping up with the rapid growth in use of social media tools, leaving their networks and endpoints vulnerable to malware infiltration. For example, how many tweets, Facebook posts or other social media communications are first processed by anti-malware tools as they enter the corporate network? As noted earlier, the research for this white paper found that 27% of organizations do not monitor use of social media, and so they simply will have no clue about how many threats are entering through this channel.

  Many organizations have been the victim of social media malware, a problem that we anticipate will increase. Using an enterprise-grade social media platform will alleviate some of these concerns, but all platforms – consumer-oriented or otherwise – must be protected against malware infiltration.

- **Monitor s content**
  Posts from social media platforms should be monitored for content that violates corporate, regulatory or legal policies. This might include scanning for content that is too sensitive or confidential to send through social media, or ethical wall violations. Monitoring is essential in heavily regulated industries, such as financial services, that have specific requirements to monitor communications with clients and others. Monitoring may occur after the fact, such as sampling employee posts to check for inappropriate content; or it might happen in real time or near real time to monitor posts before they leave the organization. While some believe

that pre-send scanning will address problems before they occur, this subverts the immediacy of social media communications, and so a reasonable, enforceable policy and effective training is a better option that preapproval.

DEPLOY AN ENTERPRISE SOCIAL SOLUTION

For most organizations, it makes sense to implement an enterprise-grade social media platform to replace and/or supplement the consumer-focused platforms that are currently in use. Enterprise-grade solutions can provide additional features and functions and can address many of the security and content management concerns that consumer-focused tools cannot, and they can significantly improve communication and collaboration between employees, business partners and others.

ARCHIVE SOCIAL MEDIA CONTENT

Finally, it is essential to log and archive all of the content that might include a business record and that could 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 information might slip through and not be retained, but this will depend to a large extent on management's tolerance for risk, the industry in which an organization operates, the 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 linked to their corporate identity.

It is important to note that archiving is quite different from simply backing up data in that all communication content is examined and indexed in a way that facilitates intelligence and granular retrieval (search-ready state) and the opportunity to apply policies for automated supervision/review on the front end. It is also important to note that most social media channel providers will take a long time to find and produce a requested message or record; this will impact the ability to respond to an audit request in a timely fashion or prepare for litigation.

It is also important to retain the context of social media posts instead of simply retaining individual posts, such as converting them into an individual communication that is saved like an email. Doing so limits the ability to search on the inherent characteristics of social media content (e.g., searching only for Facebook updates) or when searching is limited to the fields of an email (e.g., sender, recipient, subject or body). Plus, social media content that is converted into an email for purposes of archiving the content turns this content into isolated blocks of text in the archive, instead of in their original conversational context. This context is essential during eDiscovery and regulatory compliance.

An important best practice in the context of archiving social media content is to use an archiving platform that can archive all relevant content types, not just email or social media. A single archive managed using a single console will enable efficiencies that a set of siloed solutions cannot provide. Plus, it will reduce the chance of not being able to find relevant information when necessary.

Considering the long term use of archived content, decision makers should also consider how data mining and analytics – essentially, the application of Big Data practices – can be applied to social media for the purpose of extracting insight and intelligence from social media content. This is essential for organizations that seek to understand their customers and prospects more thoroughly.

SPONSOR OF THIS WHITE PAPER

Proofpoint is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive archiving, compliance, eDiscovery and governance. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system for business critical records. Proofpoint offers a proven, next-generation archive solution that leverages cloud intelligence for deep insight into your data to reduce cost, complexity and risk.

proofpoint™

www.proofpoint.com

@Proofpoint_Inc

+1 408 517 4710

REFERENCES

[i] http://www.slideshare.net/mrdosoqi/maher-dosoqi-arketingtipssocialmediastats201525012015

[ii] Osterman Research survey of end users, January 2016

[iii] http://www.cnbc.com/2015/04/22/facebook-earnings-42-cents-per-share-vs-expected-eps-of-40-cents.html

[iv] http://www.reuters.com/article/us-facebook-finra-idUSBRE98F0TZ20130916

[v] http://www.gibsondunn.com/publications/Pages/2015-Mid-Year-E-Discovery-Update.aspx#social

[vi] *Calvert v. Red Robin International, Inc.*, No. C 11-03026 WHA, United States District Court, N.D. California

[vii] http://www.wired.com/2012/07/how-companies-accidentally-leak-their-own-products/

[viii] http://www.wired.com/2012/07/how-companies-accidentally-leak-their-own-products/

[ix] http://www.managementtoday.co.uk/news/1323688/twitters-cfo-accidentally-tweets-its-secret-m-a-plan/

[x] http://www.socialmediatoday.com/content/business-hazards-online-oversharing?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=Social%20Media%20Today%20%28all%20posts%29

[xi] http://www.databreachtoday.com/twitter-state-sponsored-attack-alerts-a-8746

[xii] http://www.techweekeurope.co.uk/e-marketing/malvertising-promoted-tweet-twitter-proofpoint-181879