WHITE PAPER

Best Practices for Archiving and Securing Social Media and Collaboration Platforms

An Osterman Research White Paper
Published November 2017

actiance®

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

OSTERMANRESEARCH

EXECUTIVE SUMMARY

The use of social media – both from "official" corporate accounts and from employees' personal accounts – is growing rapidly. Most organizations and their employees are using a large and growing number of social media tools for a variety of purposes, some of which are related to their work and some used for strictly personal reasons. Add to this the growing number of enterprise-grade social media and collaboration tools that IT and other departments are deploying to improve work processes, enable enhanced employee productivity, and provide more efficient file sharing and communication between employees.

However, while beneficial, the use of these tools comes with significant risk on two levels:

- In many organizations, critical business content generated by and stored in both enterprise-grade and non-enterprise social media accounts is not being properly archived and retained, exposing organizations to a variety of risks. These include an inability to satisfy regulatory obligations, an inability to place important business content on legal hold, and an inability to discover and produce information during litigation.

- Unmanaged social media and collaboration solutions can serve as a conduit for ransomware, other malware and data breaches, and they are an effective method for cyber criminals to use social engineering techniques as an attack vector. Although more traditional tools like corporate email are typically well protected against threats like these, social media and collaboration tools very often are not.

The key for any organization is to enable the use of social media and collaborative tools and gain from the productivity and other benefits they provide, while at the same time properly managing these tools and the content they generate and mitigating the risks they can introduce.

KEY TAKEAWAYS

- Social media use, both approved and unapproved, is growing at a healthy pace in most organizations.

- The vast majority of organizations have well-established policies in place for corporate email, but these types of policies are much less common for tools like consumer-focused social media, collaboration systems, unified communications systems and other social platforms.

- A large number of organizations have experienced a malware infection through a social media channel, most commonly through Facebook.

- Non-enterprise social media tools are unlikely to secure and protect account access and content to degree necessary to satisfy corporate security policies.

- Most organizations do not retain social media content from non-enterprise accounts, and fewer than three in five do so for social media content from enterprise accounts. Neither is content from collaboration systems retained to the same degree as more commonly used tools like collaboration solutions.

- While true archiving is quite common for corporate systems like email and file shares, it is less common for social media, text messages and other types of content, despite that these solutions often contain important business information.

- There are a number of important best practices that any organization should consider and implement in the context of proper social media management. These include understanding why social media and collaboration tools are used,

Business content generated by and stored in both enterprise-grade and non-enterprise social media accounts is not being properly archived and retained.

development of detailed and thorough policies, monitoring and managing employee use of these tools, archiving business content from them, and deploying enterprise-grade alternatives where possible.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Actiance – information on the company is provided at the end of this paper.

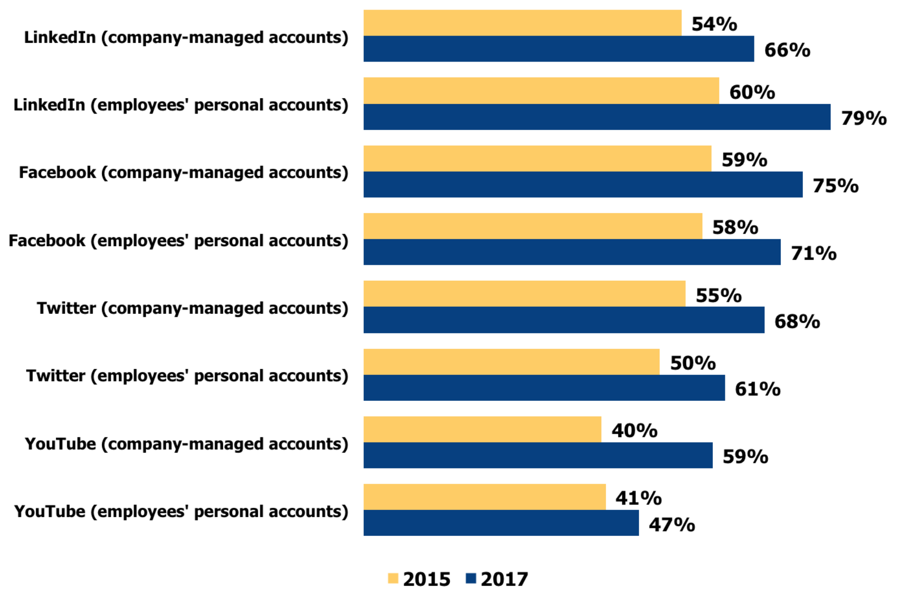
THE GROWING USE OF SOCIAL MEDIA AND COLLABORATIVE PLATFORMS

The penetration and growth of social media on a worldwide basis is truly staggering: of the global population of 7.48 billion, 2.79 billion (37 percent) are active social media users and 2.55 billion (34 percent) are active users of social media on a mobile device. As of January 2017, year-on-year growth of active social media users was 21 percent, or 482 million additional users; and the number of social media users on a mobile device increased by 30 percent, or 581 million users[i]. Facebook continues to be the most popular social media platform with 2.1 billion users as of September 2017, but other social media properties also have enormous users bases, including YouTube (1.5 billion users), WhatsApp (1.3 billion users), Facebook Messenger (1.3 billion), WeChat (963 million), QQ (850 million) and Instagram (700 million)[ii].

SOCIAL MEDIA USE IN A BUSINESS CONTEXT

Our research shows that LinkedIn is the most popular of the social media properties in the workplace that could be considered "non-enterprise", followed by Facebook, Twitter and YouTube, as shown in Figure 1. Moreover, growth of these properties for both company-managed and personally-managed accounts in the workplace has increased significantly over the past two years.

Figure 1
Penetration of Social Media in Mid-Sized and Large Organizations
2015 and 2017



Source: Osterman Research, Inc.

While we do not consider LinkedIn to be a true enterprise-grade social media property like Slack or Yammer, for example, it is perhaps the most business-focused social media tool by virtue of its extensive use in a business context. Many employees use LinkedIn in the workplace for personal networking and to search for job opportunities. It can be an effective way to find business partners and other contacts that are useful for reasons other than personal. Facebook, on the other hand, is used widely as a marketing tool by corporate marketing or branding teams in business-to-consumer applications, often generating more traffic than traditional web sites, particularly for consumer-facing brands. LinkedIn blurs the line between personal professional content/contacts and enterprise content/contacts.

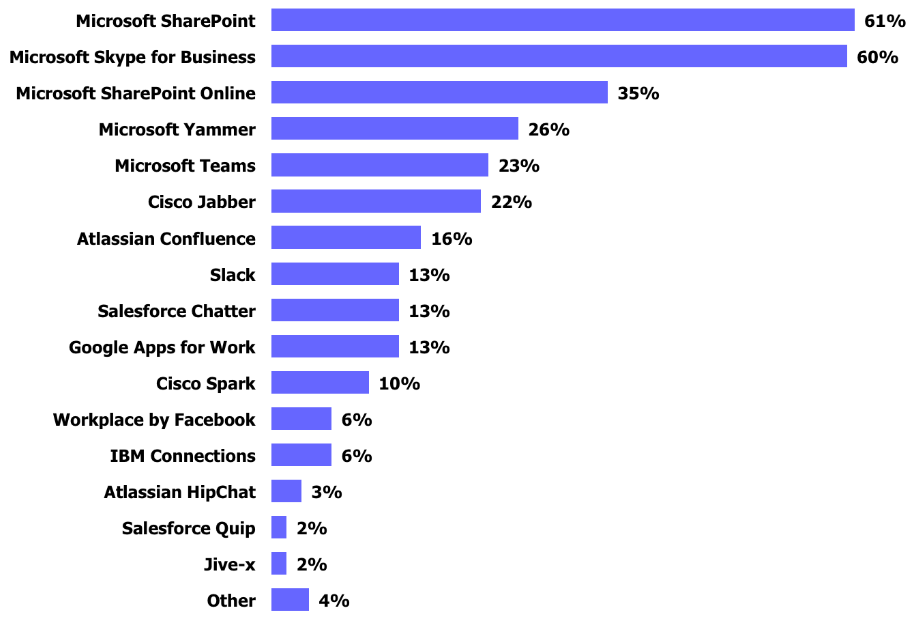
The use of Twitter continues to grow and offers potential as a tool in the context of understanding customer behavior, sentiment analysis, discovering trends among potential customers and for other purposes. The sheer volume of data generated on Twitter can be a valuable source of content for marketers and others that need to understand their brand or their business using non-traditional methods. Twitter is an excellent platform for sharing immediate and timely news, event updates, and commentary.

COLLABORATION PLATFORMS ARE BECOMING MORE COMMON

Enterprise-grade collaboration platforms are already widely used by many organizations. As shown in Figure 2, Microsoft SharePoint and Microsoft Teams (formerly Skype for Business) are the most commonly used among the organizations surveyed for this white paper, but a number of other platforms are also widely adopted. In large part, because of the dominance of Microsoft on the desktop and increasingly in the cloud via Office 365, Microsoft collaboration offerings are the five most common platforms used among those surveyed.

Enterprise-grade collaboration platforms are already widely used by many organizations.

Figure 2
Penetration of Enterprise-Grade Collaboration Platforms



Source: Osterman Research, Inc.

DRIVERS FOR THE USE OF SOCIAL MEDIA AND COLLABORATION PLATFORMS

A number of factors are driving the adoption of social media and collaboration platforms:

- Social media and collaboration can offer an avenue for information sharing and gathering that is not possible with other corporate tools like email. If decision makers are willing to create the right environment and view social networking and collaboration as an enabler of their corporate culture, it can help improve corporate decision-making. Social media and collaboration tools can improve the speed and quality of customer service, and improve the ability and desire of employees to collaborate more effectively, all resulting in improvements in many areas of the business.

- Properly configured and managed social media has the potential to create a strong sense of community for employees, business partners and others across geographic or departmental boundaries. The result is that enterprise social software and collaboration tools will be more widely used than they are today, at least among organizations with a corporate culture that supports information sharing and collaboration.

- Social media use, in particular, is being driven by its ability to provide near real time customer support, its utility as a crowdsourcing and problem-solving tool, and the fact that social media and collaboration content can be used to better understand employee and customer sentiment.

WHAT DOES THE FUTURE HOLD?

Social media use is increasing at a brisk pace, as shown in Figure 1. The research conducted for this white paper found that 56 percent of the organizations surveyed report that the use of non-enterprise social media has increased over the past 12 months, and 41 percent report it has stayed about the same. Only three percent of those surveyed report a decrease.

Osterman Research believes that the growth of social media and collaboration tools in a workplace context is driven by the growing acceptance of social media by senior management in most firms today, its utility for enabling collaboration that traditional tools cannot satisfy, gathering information that would be difficult to find in other venues, and its personal acceptance by employees.

Moreover, Osterman Research anticipates three important trends in the development of social media 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, again as evidenced by the data shown in Figure 1.

- The use of enterprise-grade social media and collaboration tools will increase significantly, but to some extent will be influenced by the choice of corporate email platform. Because email continues to be the primary communication and file-sharing tool in most organizations, Osterman Research anticipates that the ability to integrate social media and collaboration tools with the corporate email platform will be a key decision in the choice of these new platforms.

- Many services, such as Salesforce, are embedding a collaboration or social media component within the service, which means there is not likely to be a single social media toolset – even if influenced by email platform. There are going to be many different types of social media tools in use across services, roles, and corporate boundaries.

For organizations that increasingly employ social media and collaboration tools, this means that their exposure to various malware and related threats will increase, as will their obligation to retain information generated by and stored in social media systems.

THE RISKS ASSOCIATED WITH SOCIAL MEDIA AND COLLABORATION

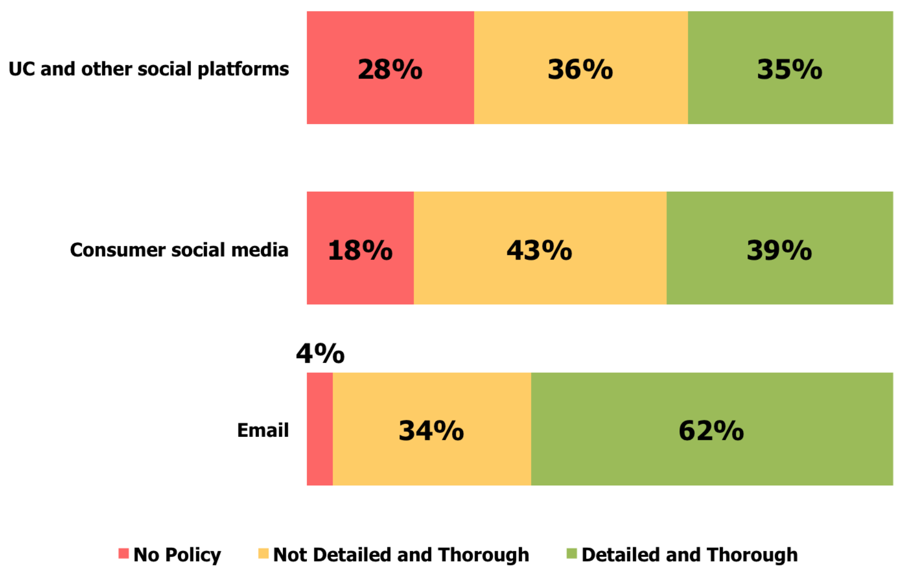
The use of social media and collaboration tools can offer numerous benefits to just about any organization, but they also introduce a number of risks with which decision makers must contend.

LACK OF ACCEPTABLE USE POLICIES

Formal policies focused on employee use of corporate email are very common, even if many of them are not detailed or thorough – our research showed only four percent of the organizations surveyed have no such email policy in place. However, as shown in Figure 3, these types of defined corporate policies are much less common for the use of consumer social media, unified communications and other social platforms used in a workplace context.

Defined corporate policies are much less common for the use of consumer social media, unified commun-ications and other social platforms.

Figure 3
Policies in Place for Various Types of Communication and Collaboration Tools



Source: Osterman Research, Inc.

Every organization should have a detailed and thorough social media policy that includes a variety of items, including the types of content that can be shared using social media, notification about the tools that are/are not permitted on the corporate network, whether or not employees can speak on behalf of their employer through social media, to what extent personal accounts can be used for business purposes, etc.

When an organization does not have a detailed and thorough social media policy – or does not have one at all -- they run the risk that data can be inadvertently leaked through social media channels. While an overt leak of information, such as sharing an embargoed product announcement, can happen in social media, there are more subtle forms of data leakage. For example, an employee who innocently tweets her travel plans, especially when traveling to the same city multiple times, might reveal that her company is in the process of doing a deal with a particular company. In the same way, an employee who tweets negative comments about clients or who posts racially or sexually harassing comments to Facebook can create legal and brand value problems. At a minimum, detailed and thorough policies should be in place to make social media behavior expectations clear.

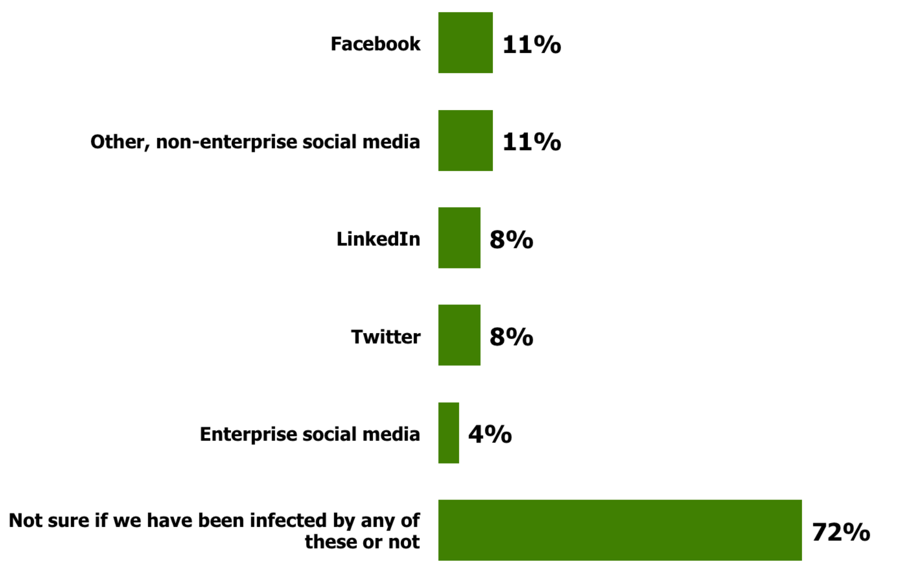
AN INGRESS POINT FOR MALWARE AND OTHER THREATS

Our research found that eight percent of those surveyed for this white paper have either had their social media accounts hacked or have been the victim of malware infiltration through social media; another six percent are not sure if either or both have occurred. Using just the data on those who have been hacked or been the victims of malware infiltration, this means that in an organization of just 500 social media users, 40 would have had their accounts hacked or served as the conduit through which malware could enter an organization.

Hacking and malware infiltration via social media and collaboration tools are becoming a more top-of-mind issue as Twitter, Facebook and other social media platforms become more widely used in the workplace. For example, cyber criminals can create bogus pages, such as a Facebook page, that will trick victims into downloading malware. Users can be tricked into these scams because the bogus pages offer something of value, such as finding out who visited their Facebook profile, and they are willing to provide their login credentials or click on a link to obtain it. Similarly, "click-jacking" can put hidden hyperlinks underneath valid content, such as Facebook ads, and then lead victims to sites that contain malware.

Although many users are not concerned about the potential for malware to enter the corporate network through social media, they should be: a large proportion of organizations have been infected by malware, as shown in Figure 4.

Figure 4
Organizations That Have Experienced a Malware Infection Through Social Media



Source: Osterman Research, Inc.

THE THREAT OF SOCIAL ENGINEERING

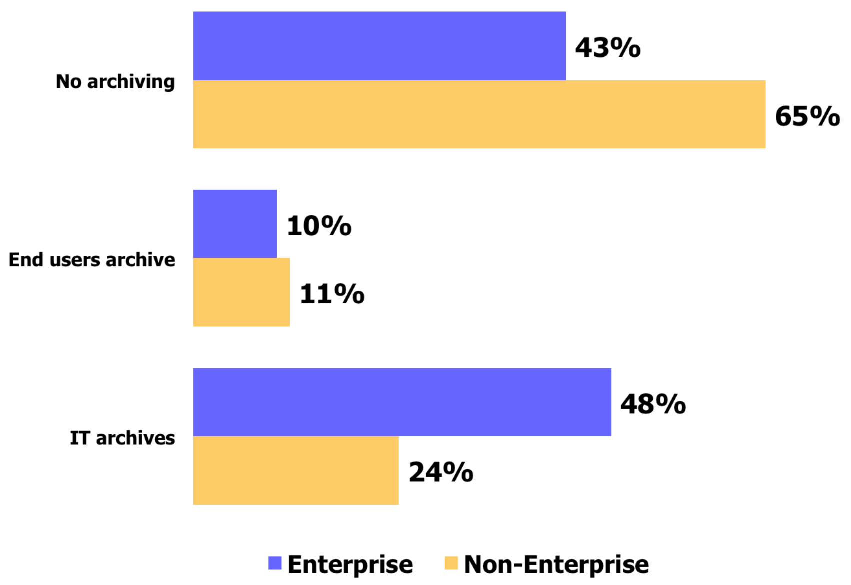
Another major area of concern in social media is social engineering in the context of social media. Many users of social media feel inherently safe when clicking on links in social media and sharing information[iii], but cyber criminals can easily take advantage of this misplaced trust. For example, cyber criminals can mine social media posts for information about potential victims that is likely to make spearphishing attempts via email more successful. Social media users will periodically be presented with a meme asking for personal information like their mother's maiden name or the name of their first pet, both pieces of information that are often used as security questions for access to web sites. Social media users will often share their travel plans, helping cyber criminals to understand when senior managers will not be in the office. Fake social media profiles can be used to spread disinformation for a variety of purposes, such as manipulating stock prices – one such scheme is alleged to have caused shareholders to lose in excess of $1.6 million[iv].

BUSINESS CONTENT IS NOT BEING RETAINED

IT retains non-enterprise social media content in only 24 percent of organizations; in 11 percent of organizations, only end users do so. However, in nearly two-thirds of organizations, no retention of non-enterprise content takes place, as shown in Figure 5. However, for enterprise-grade social media, the proportion of organizations retaining it is significantly higher: in nearly one-half of organizations, IT retains this content and in another 10 percent end users do so.

However, true archiving (indexing, tamper-proof storage and search) of social media and collaboration content is still substantially below that of other types of business content, such as emails and files, as shown in Figure 6 on the next page.

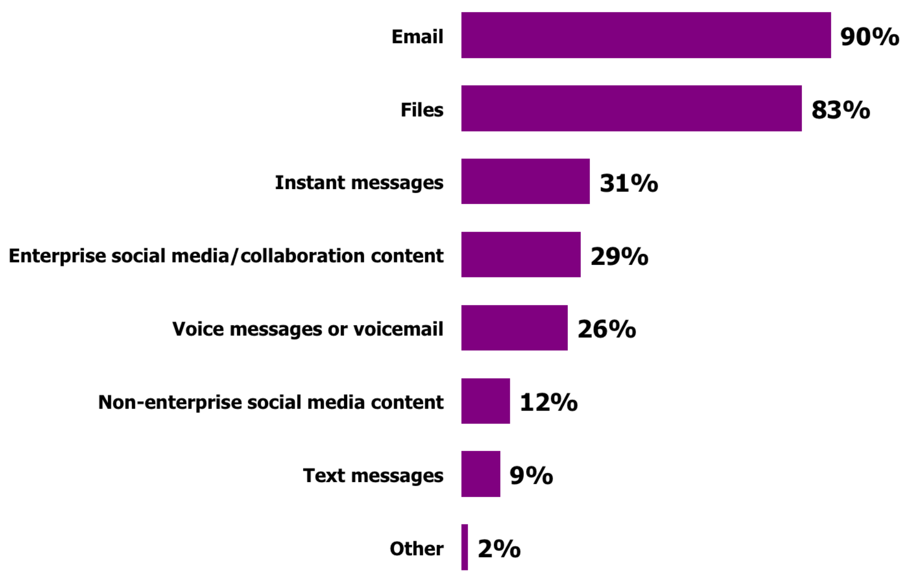
Figure 5
Retention of Social Media Content



Source: Osterman Research, Inc.

Many users of social media feel inherently safe when clicking on links in social media and sharing information, but cyber criminals can easily take advantage of this misplaced trust.

Figure 6
Percentage of Organizations Archiving Various Types of Content



Source: Osterman Research, Inc.

Many decision makers are not familiar with their regulatory obligations to retain social media and collaboration content, but a failure to retain this content can result in serious consequences for organizations even outside of heavily regulated industries like financial services, healthcare or life sciences. While most of the organizations that are performing robust social media management and control are today in the financial services industry, there is growing expansion of social media management into other regulated industries, as well. The benefits of archiving and governing social media are present even for non-regulated corporations in terms of security, search and retrieval, as well as eDiscovery and legal hold.

ARCHIVING IS ESSENTIAL

Social media and collaboration systems often contain business content that organizations should retain, just like they retain this content in corporate email and other electronic systems. Retention of all business content, regardless of the platform that created it, is part of good information governance and is necessary for both regulatory and legal reasons. For example:

- The Financial Industry Regulatory Authority (FINRA) Regulatory Notice 10-06 (January 2010) requires 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 records of those communications as required by Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 and NASD Rule 3110."[v] FINRA Regulatory Notice 11-39 (August 2011) reminded regulated firms about "the recordkeeping, suitability, supervision and content requirements for [social media] communications.[vi]"

- IIROC Regulatory Notice 11–0349 and IIROC Rule 29.7 IIROC Regulatory Notice 11–0349 (Dec. 2011) from the Investment Industry Regulatory Organization of Canada (IIROC) addresses recordkeeping and supervision requirements of communication on social media websites. In addition, all methods used to communicate, including social media, blogs and chat rooms, are subject to IIROC Dealer Member Rules. IIROC Rule 29.7 is the recordkeeping requirement, which requires firms to archive, monitor, and review electronic advertisements, sales literature and correspondence for clients, including communication on social media sites such as Facebook and Twitter. IIROC 29.7 and Regulatory Notice 11-0349 require that firms establish written supervisory procedures, as well as training and monitoring systems for social media communications.

- In 2017, a former banker with the firm of Jefferies Group LLC was fined £37,198 by the Financial Conduct Authority (FCA) for employing WhatsApp to share with a friend confidential data about two of Jefferies' clients. (WhatsApp provides end-to-end encryption between recipient and sender, which is not considered a best practice in highly regulated firms.) Although the banker was not alleged to have profited from sharing the information, the FCA sought to impose a heavy fine in this case. Perhaps in response to this case, Deutsche Bank AG has now prohibited the use of WhatsApp and other text messaging and chat apps for all work-related communications within the company. The bank made this decision because it did not think it could archive this type of content properly.

- Social media is required for production in many legal cases, such as:

    - *Pugh v. Junqing*[vii], in which the plaintiff requested from the defendant "all social media (including, but not limited to, Facebook, Twitter, LinkedIn, Google+, Tumblr, and YouTube), social networking, blog, and/or internet postings, photographs, uploads, messages, updates, events, and/or entries by Defendant in the 12-hour period immediately before and after the subject wreck." The court granted the motion, but narrowed the request to "all social media content which has any relevance to this case."[viii]

    - *Ferraro v. Hewlett-Packard Co.*[ix], in which it appears a judge took the number of "likes" on a Facebook fan page into consideration in making a ruling about the appropriate use of a laptop[x].

    - *Ehrenberg v. State Farm Mut. Auto. Ins. Co.*[xi], in which the defendant's insurance provider sought to conduct discovery on a plaintiff's Twitter, Facebook and Instagram accounts. Although limits were placed on the defendant's request for discovery, the court agreed that this content could be searched for posts and images related to the accident that was the subject of the case, as well as other relevant information[xii].

What is an employer's responsibility in the context of preserving relevant information?

WHAT ARE EMPLOYERS' RESPONSIBILITIES?

Although many organizations do not archive corporate social media content like Facebook posts or tweets, and even fewer archive the social media posts from employees' personal accounts, there are some important use cases to consider. For example, if an employee is terminated for making an offensive post on a non-work-related social media page, the employer must be prepared to defend itself in a potential wrongful termination suit. For example:

- An individual who worked for a non-profit organization was terminated because of an image she posted on Facebook mocking the Tomb of the Unknown Soldier at Arlington National Cemetery[xiii]. A salesperson at a BMW dealership was fired for posts that disparaged his employer and its customers[xiv]. In both cases, the firings were deemed to be appropriate and not protected speech.

- Five employees were terminated after they posted to Facebook about one of their co-workers who was going to complain about their work performance to the management of the organization. However, the National Labor Relations Board (NLRB) ruled that they were fired wrongfully because their speech is considered to be a "concerted activity" and therefore protected[xv].

The key question then becomes, what is an employer's responsibility in the context of preserving relevant information in cases like these? There are a number of activities that the NLRB considers not to be "fireable" offenses[xvi]. However, there are posts that employees can make on social media that will permit their employer to terminate them. Any organization faced with this type of situation should preserve all of the relevant social media posts that are available, including the employee's posts that are determined to be offensive. This should include the date, time and any other metadata associated with the posts; any comments that are related to the post; and all other information that can offer context about the offending information. This might include employee admissions that their post was genuine and not the result of a hacked account, any explanations they offered as to why they chose to post the information, and anything else that may help an employer justify their decision to retain or terminate the employee. Archiving all of the relevant information and its context is essential in justifying the decision to terminate and to protect the organization from any litigation it might face as a result.

USING SOCIAL MEDIA FOR HIRING DECISIONS

Many employers use social media content to evaluate prospective employees and will reject applicants based on objectionable content they find in those posts. However, because Title VII of the Civil Rights Act of 1964 prohibits employers from discriminating against prospective employees based on their race, color, religion, sex, pregnancy or national origin[xvii], if a hiring manager considers social media content that may include references to a potential employee's national origin or their participation in a gender-based organization, for example, they must prove that this "off-limits" information was not considered if the individual is not hired.

Consequently, employers should take a two-step approach to using social media content for evaluating candidates: 1) have someone not involved in hiring decisions cull unusable information from prospects' social media streams, and 2) deliver only the culled information to HR for their evaluation. The creation of an "ethical wall" in this manner can protect employers from claims that social media information was used in an illegal way. Moreover, HR should archive this content so that it can defend itself against allegations of illegal hiring practices. Archiving social media content will probably not fully insulate the employer from charges of illegal hiring practices, but it can demonstrate compliance with the law.

The key is that even if a specific regulatory or other obligation to retain social media content does not exist, firms should seriously consider doing so as a means of protecting the organization and managing the risk it faces from the growing use of social media, both corporate-sanctioned and personal.

ALSO CONSIDER THE GDPR

The General Data Protection Regulation (GDPR) is the newly harmonized, European-wide regulation that mandates the protection of data about residents of the European Union (EU). It applies to every organization that controls or processes data on people in the EU, regardless of where that organization is located. It updates, replaces, and extends the protections previously afforded through the earlier 1995 directive on data privacy (Directive 95/46/EC), and will go into effect on May 25, 2018.

The GDPR is important in the context of archiving and security of all data types – including social media and collaboration system data – for several reasons:

- It applies to most organizations worldwide. If an organization controls or processes data on people living in the EU – even if the organization is not located in a member state – it still applies.

- It imposes significant penalties in the form of enormous regulatory fines for non-compliance. If an organization meets the test of applicability for the GDPR, it cannot opt out of complying.

- It touches every data process in organizations that collect or process personal data, and it covers both direct and indirect data identifiers in every data system.

- It forces organizations to know and understand their data from a 360-degree perspective. Organizations that process EU citizen data will need to know where it is being processed, who is processing and storing it, and they must demonstrate the ability of "erasure" on it no matter where it lives. This includes things like social media posts that an organization has archived.

- It demands greater transparency with people on how their data is collected and processed, and introduces notification requirements when personal data is breached. There are reputational consequences of getting this wrong, particularly in light of the fact that during the previous 12 months, 47 percent of the organizations surveyed by Osterman Research have suffered a breach of customers' or other personal data, employees' personal data, corporate intellectual property, or other sensitive or confidential information.

- Under the GDPR, in most cases data controllers and processors cannot charge for requests from data subjects, which means that it is now more likely that many more individuals will be making demands about the information that is held about them.

- Organizations are running out of time to become compliant with the GDPR: as of the publication of this white paper, there is less than six months until the regulation goes into effect.

BEST PRACTICES TO CONSIDER

Osterman Research recommends a number of best practices to properly manage social media and collaboration tools.

UNDERSTAND WHY THE TOOLS ARE USED

To properly manage social media, the initial step for decision makers should be to understand fully how social media and collaboration tools are used in the organization, since this will determine the level and types of effort, policy and technology required to manage them. For example, decision makers should ask the following questions of key stakeholders:

- Are personally managed social media tools used to send business content, such as links to corporate documents?

- Is social media used for informal, non-business-related communications among employees using their personal social media accounts on their own devices?

- Is the marketing team using social media to communicate corporate messages, such as offers, announcements or other company information?

- How is social media used on company-owned devices?

- Are employees using social media to communicate with prospects, clients or business partners? If so, is this being done via personal and/or corporate accounts?

- How are social media posts governed by various regulations or laws?

- Has any sort of return-on-investment analysis been created to determine how, where and why social media should be used?

- Is the organization monitoring social conversations that affect the brand/company, and is there an opportunity for the organization to join the dialogue?

To properly manage social media, the initial step for decision makers should be to understand fully how social media and collaboration tools are used.

- How is the social media tool accessed – via a web site, desktop app, mobile phone app?

The right answers to these questions are essential in order to determine how to create policies and the most appropriate technologies to implement. For example, if social media is used by employees only for informal and/or personal communications using their own devices with their own accounts, archiving of this content is normally not necessary (or even possible) in most cases. However, if the marketing group is sending corporate messages via company-supplied platforms, it's important that monitoring and archiving technologies be deployed to ensure that all relevant content is properly managed and retained. The same applies to things like sales-related conversations that take place with customers and prospects using personal accounts.

DEVELOP DETAILED AND THOROUGH POLICIES

Next, decision makers need to determine how to implement policies that will focus on developing the right balance between employees' freedom to gather information and communicate via social media, compliance with industry regulations, the business benefits that will be realized from the use of social media tools, and advice from legal counsel.

Decision makers should consider developing a social media policy regardless of whether or not the company chooses to use non-enterprise tools like Facebook, or an enterprise-grade social media solution. This policy should:

- **Be integrated with the organization's overall communications policies**
  Social media policies should be an integral part of an overall set of communication policies that govern the use of corporate email, instant messaging tools, personal Webmail, collaboration tools, cloud-based storage repositories, personal file-sync-and share tools, and any other capability through which individuals might share corporate information.

- **Define the acceptable use of social media**
  Social media policies should include provisions focused on appropriate use of social media tools, including any requirements that prohibit posting of offensive comments or images, defamation of competitors or slandering of individuals, customer content, content that could violate laws or the publication of confidential information, links to inappropriate Web sites, posts in bad taste; etc.

- **Clearly state the right to monitor social media communications**
  Social media policies should clearly state that corporate management reserves the right to monitor employee communication and list the circumstances under which management has the right to act on this information. Employees should also be aware that their content transiting corporate infrastructure may be retained indefinitely.

- **Make the policies granular**
  Social media policies should be granular so that different roles can be subject to different policies. For example, senior managers generally need to be governed by different policies when communicating with external auditors versus communicating with employees. Broker-dealers should be subject to different social media rules than their firm's clerical staff. Formal communications from senior decision makers should be subject to different monitoring and review practices than those generated by employees' personal tools.

- **Identify acceptable and unacceptable social media tools**
  The social media tools that are approved and not approved for business purposes should be specified in a corporate policy, preferably offering a rationale for the decision. This includes the social media sites or tools themselves, as well as the devices on which these sites are accessed – smartphones, tablets, home computers, work computers, etc. While some decision makers may opt for a strict approach and create policies that prohibit the use of non-enterprise social

media tools or other capabilities on corporate infrastructure, this draconian approach will probably not work and will simply prompt employees to use their personal devices to access these tools while at work. Instead, an approach that permits appropriate use of these tools will better 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 capture this content in most cases. There should be a process in place for vetting, evaluating and approving new social channels that employees would like to use.

- **Determine who owns social media contacts**
  Clear succession planning should be a part of any social media policy. For example, when an employee leaves the organization, the corporate policy should help decision makers determine who "owns" his or her followers or friends. For example, are an employee's corporate Facebook posts the property of his or her employer if they were posted during work hours? Do followers on Twitter belong to the employer or employee? Do relationships with corporate customers on LinkedIn belong to the employer or employee?

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

- **Establish response processes for data breaches**
  Policies should clearly state the consequences of a policy violation. For example, if an employee accidentally tweets a product announcement a day before a press release is issued, or mistakenly posts trade secrets, the consequences of these actions should be clearly spelled out just like they would be for any other type of data breach.

Policies should be implemented in such a way that significant employee buy-in can be achieved, since unreasonable policies won't be followed. Plus, it is essential to continually revisit and update these policies on a regular basis to keep them up-to-date with new social media capabilities, regulations, laws and best practices.

Policies should be implemented in such a way that significant employee buy-in can be achieved.

MONITOR AND MANAGE EMPLOYEE USE OF THESE TOOLS

Every organization should deploy the appropriate technologies that monitor social media posts for policy violations and protect against malware with a mindset of being proactive rather than merely addressing problems after they occur:

- **Mitigate the impact of social engineering**
  Users need to be educated about the negative effects of social media, including oversharing of information that can be used by cyber criminals, indiscriminately clicking on links or advertisements in social media posts, or accepting "friend" requests from unknown individuals. Moreover, it's a good idea to deploy solutions that will block potentially dangerous content from the social media interface, such as advertisements or games.

- **Scan for malware**
  Threats that can enter an organization through social media, such as malicious links in tweets or ads in Facebook, need to be blocked. This is especially 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.

  A fundamental problem with social media is that these tools are normally less well defended by most organizations than more mainstream tools like corporate email. Many IT departments are having difficulty keeping up with the rapid growth in use of social media tools, leaving organizations vulnerable to malware infiltration. Most tweets, Facebook posts and other social media content are not processed by anti-malware scanning tools as they enter the corporate network.

A large proportion of organizations have been the victim of social media malware and growth of this problem will only increase. Using an enterprise-grade social media platform will alleviate many of these concerns, but all platforms – consumer-focused or otherwise – must be protected against malware infiltration.

- **Restrict access and monitor outbound content**
  Every social media protocol that might be employed should be restricted from use for some roles and monitored for content that violates corporate policy. If users in specific roles do not need to use it, then they should be restricted from access. If users have access, monitoring can include looking for content that is too sensitive or confidential to send through social media, scanning for potential data breaches, or ethical wall violations. Monitoring is especially important in heavily regulated industries, such as financial services or healthcare, that have specific requirements to evaluate communications. Monitoring may occur after the fact, such as sampling employee posts to check for inappropriate content; or it could happen in real time or near real time to monitor posts prior to their being sent.

ARCHIVE BUSINESS CONTENT FROM THESE TOOLS

An archive and log of all of the critical content in social media and collaboration tools should be maintained. It's normally easier to archive or log all social media content than take the risk that some important content might be missed, 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. A key part of content archiving and 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. It is also important to retain the context of social media posts instead of just monitoring them.

Decision makers need to remember that business information in text messages must also be archived – for example, FINRA has determined that information sent via text messages must be retained like other electronic communications[xviii]. A legal hold placed on data generated and stored on mobile devices will normally be more difficult than for data taken from conventional, IT-managed platforms like corporate email. Some organizations notify employees of their need to hold data, but this is not an effective means of ensuring that a legal hold actually takes place, and so archival of text messages and other content is essential.

It is very important to consider deployment of an archiving solution that can archive multiple content types, not just email or social media. A single archive managed via a single interface will enable efficiencies that a set of siloed solutions cannot provide, and it will reduce the likelihood of not finding relevant information when necessary.

An archiving solution that archives social media content should not "convert" social media posts into the body of an email such that content or context is lost. Conversion can limit the ability to search on the inherent characteristics of social media content (e.g., searching only for Facebook updates) when querying is limited to the fields of an email. Further, social media content shoehorned into an email format runs the risk of rendering like standalone blocks of text in the archive, rather than in their proper conversational context. This context can be important for eDiscovery and regulatory compliance.

It is also important to consider how data mining and analytics can be applied to social media for the purpose of extracting business intelligence from social media content. This is especially important for organizations that want to understand their customers and prospects more thoroughly.

DEPLOY ENTERPRISE-GRADE SOLUTIONS

Finally, decision makers should seriously consider deploying an enterprise-grade social media or collaboration solution to replace the non-enterprise tools that are currently in use. Enterprise-grade tools can provide additional features and functions and can address many of the security and archiving concerns that consumer-focused tools cannot.

SPONSOR OF THIS REPORT

Actiance is the leader in communications compliance, archiving, and analytics. We provide compliance across the broadest set of communications and social channels with insights on what's being captured. Actiance customers manage over 500 million daily conversations across 80 channels and growing. Customers include the top 10 U.S., top 5 Canadian, top 8 European, and top 3 Asian banks. The Actiance advantage is customers stay ahead of compliance and uncover patterns and relationships hidden within their data. Learn more at www.actiance.com. Actiance headquarters are in Redwood City, California. For more information, visit www.actiance.com or call 1-888-349-3223.

actiance®

www.actiance.com

@Actiance

+1 888 349 3223

sales@actiance.com

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

[i] Source: Data gathered by Hootsuite (https://blog.hootsuite.com/social-media-statistics-for-social-media-managers/)

[ii] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[iii] Wombat Security's *2017 User Risk Report* found that 57 percent of US respondents are under the impression that business-focused social media pages are approved by the social media property on which they appear.

[iv] https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/scottish-citizen-indicted-for-twitter-based-stock-manipulation-scheme

[v] https://www.finra.org/Industry/Regulation/Notices/2010/P120760

[vi] https://www.finra.org/sites/default/files/NoticeDocument/p124186.pdf

[vii] *Pugh v. Junqing*, U.S. Dist. LEXIS 164456, at *5-6 (E.D. Mo. Oct. 4, 2017)

[viii] http://bowtielaw.com/2017/11/02/remember-to-propound-narrowly-tailored-requests-for-social-media/

[ix] *Ferraro v. Hewlett-Packard Co.,* 2013 U.S. App. LEXIS 13569, 12-13 (7th Cir. Ill. July 3, 2013)

[x] http://bowtielaw.com/2013/07/17/did-the-court-just-look-at-facebook-on-its-own/

[xi] *Ehrenberg v. State Farm Mut. Auto. Ins. Co.*, No. 16-17269, 2017 U.S. Dist. LEXIS 132036, at *3 (E.D. La. Aug. 18, 2017)

[xii] http://bowtielaw.com/2017/08/21/proportional-social-media-requests-for-production/

[xiii] http://gawker.com/5962796/happy-now-good-employee-lindsey-stone-fired-over-facebook-photo

[xiv] http://www.employmentlawblog.info/2017/03/can-you-be-fired-for-political-social-media-posts.shtml

[xv] http://www.employmentlawblog.info/2017/03/can-you-be-fired-for-political-social-media-posts.shtml

[xvi] http://socialmediatoday.com/mike-allton/1247406/why-you-cant-fire-employees-complaining-facebook

[xvii] http://www.eeoc.gov/facts/qanda.html

[xviii] https://www.forbes.com/sites/joannabelbey/2017/04/19/finra-and-social-media-what-to-expect-from-new-guidance/#6e92c0574a6e