The Use of Social Media in the Workplace

Written for KAMIND, IT, Inc.

By Ravi Das

Introduction

Gone are the days when a business would have to spend hundreds of thousands of dollars on both radio and television ads in order to showcase their new products and services. In most cases, trying to compute the Return On Investment (ROI) would be a nearly impossible task. Fast forward to today. Now, all that a marketing team needs to do is simply create a fancy video, put in the right slogans and keywords in the script, and upload it to YouTube.

Within just a couple of minutes, this video has the potential to go "viral" and reach millions of people worldwide. The only costs that would be associated with it is the development of the video, which would be just a mere fraction of what it would take under the traditional means, as just described. But keep in mind that YouTube is not the only other social media outlet that is available for this purpose.

There are the likes of Facebook, Twitter, LinkedIn, Instagram, Pinterest, etc. On these platforms as well, a business can post thought-provoking articles and micro-blogs not only about their products and services but also the key happenings that are taking place in their industry. No need to send out snail mail blasts, a marketer can just use these tools, and best of all they are free.

In fact, the use of social media tools is fast becoming one of the vehicles in which Corporate America is using to reach out not to only their customers and prospects, but even to their employees as well. Although these avenues possess great advantages, they also possess a great deal of unknowns as well, especially when it comes to Cybersecurity.

Therefore, just like having a security policy or even a disaster recovery plan in place, it is very important to also have a social media policy in place, so that your company can remain safe. This is the objective of this whitepaper.

The Cybersecurity Risks of Social Media

When one thinks of a Cyberattack, very often, the image of a hacker going after servers and databases in order to gain the Personal Identifiable Information (PII) and other types of confidential data very often comes to mind. But this is only one way of getting these proverbial "crown jewels". The other way is to also keep tabs on the social media activity of a particular company in an effort to determine their weakest and most vulnerable spots.

For example, whether they have a malicious intent or not, employees are very often negligent as to the content that they are posting on their company's social media sites. Although he or she may not put up the Social Security and Credit Card numbers of their customers, they can often put up content that over time, can constitute a company's profile, and how the employees and management interact with another, and other external entities.

The Cyberattacker can then put together all of these pieces of content, and from there, get an entire picture of the organization in question. From here, he or she can then use the principles of Social Engineering in order gain a foothold into the business, and from there, launch their threat vectors. Or, if there is a known vulnerability in a particular Social Media site (Facebook has been so far the most notorious in this aspect) the Cyberattacker can just penetrate into that fairly easily to get the company's IT Assets.

But regardless of a how a Cyberattacker uses the Social Media tools to gain access to an unknown back door, they all are prone to a number of key threat vectors, which in turn, can make a business suffer from a security breach. They are as follows:

1) Unused Social Media Accounts:

   Because Social Media accounts are free to set up, there is a strong temptation amongst all the departments within an organization to set up their own individual accounts, in order to reach to both prospects and existing customers. Or, as mentioned previously, these various Social Media sites can also be used for internal communications with employees. But very often, many of these accounts can go unused for very long periods of time, and even become inactive. Just like for examining for open ports that are not in use on a Network Infrastructure, a Cyberattacker can also probe for these unused Social Media accounts in order to gain a point of entry into the organization.

2) Employee Error:

   When employees post content up about a new product or service, there is often an excitement in the rush to post up as many links as possible that are related to it. But in this heat of the moment, there is a high statistical probability that they could put up a proprietary link that they did not mean to. But the fact remains that this link has been made open to the public, and the Cyberattacker will always have their eyes and ears open to this. In this case, once this has been discovered, it will be too late, as the damage has been done. In fact, one study has even discovered that 77% of employees have put up a wrong link, by sheer mistake.

   (SOURCE: 1).

3) Third-Party Applications:

   Even if you are authorized to download mobile apps onto your company issued wireless device (such as a Smartphone), the Cyberattacker will always find a way in which to penetrate them in order to gain access to not only the company's Social Media accounts, but even your personal ones as well, in order to hijack your password and other relevant login data.

4) Phishing and Malware:

   When one thinks of these two, very often the first thing that comes to mind is either clicking on a malicious link or downloading an attachment in an Email message that contains some kind of Malware (such as those. DOC and .XLS file extensions). But keep in mind that the Cyberattacker of today can even hijack a legitimate Social Media account and even put up a posting with a link attached to that will take you to a spoofed website. In this regard, once again, Facebook has been the prime target here, with accounts being hijacked on an almost daily basis, and illegitimate postings being put up. In fact, nearly 2/3 adults in the United States know that their Social Media accounts have been hacked into, but still do nothing about it.

   (SOURCE: 2).

5) Establishing Fake or Impostor Accounts:

A Cyberattacker does not necessarily have to hack into an existing social media account in order to hijack passwords or even put Phishing related posts. All he or she can also do is simply create a fake or phony account, and make it look like the real thing. For example, these kinds of accounts can be used to target both customers and employees simultaneously, in order to con them into giving up their Personal Identifiable Information (PII) or company secrets, respectively. In fact, the setting up of fake Social Media accounts has increased by two-fold just within the last year, because they are so hard to detect.

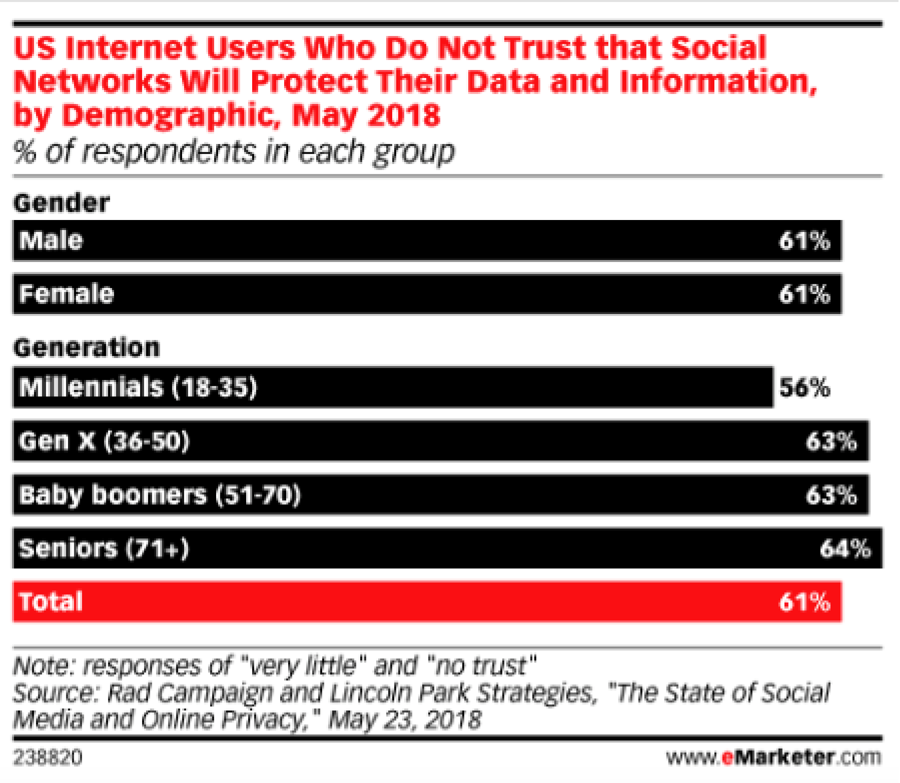
(SOURCE: 1).

6) Breaking Into The Privacy Settings:

Although the major Social Media sites have claimed that they have beefed up their privacy settings so that confidential remains that way, many companies and users still have no faith in this. In fact, according to a recent survey, many of the respondents claim that virtually have no trust in the privacy settings in the Social Media Sites that they make the most of.

(SOURCE: 3).

This is also further illustrated in the diagram below:



US Internet Users Who Do Not Trust that Social Networks Will Protect Their Data and Information, by Demographic, May 2018

% of respondents in each group

Note: responses of "very little" and "no trust"
Source: Rad Campaign and Lincoln Park Strategies, "The State of Social Media and Online Privacy," May 23, 2018

238820 www.eMarketer.com

(SOURCE: 1).

7) Shared User Access and Interconnected Mobile Apps:

In Corporate America today, many departments (such as of IT, Marketing, Accounting, Finance, Human Resources, etc.) typically share passwords across those applications and systems that are interconnected with another. A perfect example of this is when the organization hires an exclusive Social Media Manager from an external third party to manage their content. Rather than having to create different passwords for each Social Media Platform, usually only one password is created merely for the sake of ease and convenience. Not only is this a grave security risk, but the fact that this administrative password is being shared with an external third party poses even a far greater concern. As mentioned, if there are other apps that are connected to these Social Media sites (such as dashboards, analytical tools, etc.) this external third party can very easily gain access to even further sensitive information and data in the company.

8) Social Media Botnets:

To some degree or another, we have all heard of "Bots". A popular example of this is the "Chatbot", which is a virtualized customer agent which can answer customer service-related questions and requests without the need for any sort of human intervention. Although this can be quite advantageous and brings many benefits with it, it can also pose a very serious security threat as well. For instance, as it relates to a Social Media account, a bot can be used to make it look like that it is a real, live person (when it is really not) that is interacting with an employee in an organization. These are known as "Socialbots". But apart from the aspect of the security threat, there are other, non-quantifiable risks that it brings as well, such as skewing tracking data, such as fake ad impressions, and even creating fake hashtags that can be used in a Phishing Attack. They can even be used to alter your customer's perceptions of your company brand.

9) Insider Attacks:

As a company grows and expands, or even offers new products and services, there is a strong tendency for both employees and management (and even the C-Suite) to share more than what is really necessary, as mentioned previously. For example, if an organization is opening up a new office, there will be a temptation to post up pictures of the insides of it and the new employees in order to further "show off" the brand on Social Media sites. It is important to keep in mind that while prospects and existing customers may be "wooed" by this, the Cyberattacker is also keeping very close tabs on it as well. But their purposes are far more nefarious in nature. For example, by getting a clear picture of what is inside the new office as well as its new employees, the Cyberattacker can use Social Engineering to lure a naïve employee into perhaps launching a covert Insider Attack in those areas that have been posted on the various Social Media Sites. In fact, in this instance, the Cyberattacker can be so stealthy into the manipulating the mindset of this particular employee that he or she may not even be aware that are participating in an Insider Attack against the very company that they work for.

What Is A Social Media Policy?

A Social Media Policy can be defined specifically as follows:

"The goal of a social media policy is to set expectations for appropriate behavior and ensure that an employee's posts will not expose the company to legal problems or public embarrassment. Such policies include directives for when an employee should identify himself as a representative of the company on a social networking website, as well as rules for what types of information can be shared. Almost all social media policies include restrictions on disclosing confidential or proprietary business secrets or anything that could influence stock prices."

(SOURCE: 4).

Breaking down this definition, a Social Media Policy serves three broad purposes:

- It sets out expectations of what both management and employees can and cannot post on Social Media sites as it relates to corporate matters;
- It clearly states how a manager, or an employee should identify their titles and position within a company without revealing any further confidential information;
- It stipulates the consequences if an employee or even a manger posts confidential and/or proprietary information and data about their organization, whether they do it knowingly or not.

Thus, as one can see, having this kind of policy in place is very crucial, especially given the fact that Social Media sites are being so heavily used for marketing persons and can go "viral" almost instantaneously. The rest of this whitepaper will examine the importance and benefits of having a Social Media Policy, the crucial components that must go into it, and examples that even you can use for your own business.

The Importance & Benefits of a Social Media Policy In Your Business

In a theoretical sense, just about any individual can create as many Social Media accounts as they want, for free. Also, there is really no limitation either as to the kind or type of content that can be posted, whether it is in the form of writing, video, audio, or pictures. But when it comes to the workplace, obviously many more restrictions need to be put into place, especially from the standpoint of Cybersecurity.

The following are some key reasons why having a Social Media Policy that is enforced on a daily basis is a must for Corporate America these days:

1) <u>You need to let your employees know what is deemed to be acceptable and what is not in the workplace</u>:

   Employees access their Social Media sites on an almost daily basis, whether it is work or personal related. Obviously, you have no control as to what they can post on their own Social Media accounts, but when it comes to work-related matters, you almost have complete control. In fact, according a recent survey, almost 80% of employees in Corporate America access some kind of Social Media platform during work hours.

   (SOURCE: 5).

   In this regard, it needs to be very carefully spelled out in great detail as to the type of content that can be posted. For example, any negative comments or connotations about the company cannot be posted. What would be acceptable is talking about new products and services, customer testimonials, content that discusses the trends that are occurring in your industry, as long as they do not give or even indirectly refer to any kind or type of confidential information/data.

2) It will protect the brand and reputation of your company:

By having a solid Social Media Policy in place, you can stipulate how and when an employee can access their Social Media sites. For example, perhaps employees should be only allowed to access their personal sites only during the lunch or break hours, or after work. But they cannot use company issued devices to access them, they have to use their own personal device in order to do this. However, during the work hours, they should be able to access company related Social Media sites, if this is part of their daily job function. But they should only use company issued devices to do this. In order to help keep track of all of this, an IT Department can very easily deploy approved and authorized Key Logging software to see if employees are abiding by these rules. It is important to keep in mind that any slip ups can easily tarnish the company brand or reputation in just a matter of minutes and trying to recover from that can literally take months to accomplish.

3) It can actually elevate your reputation in the marketplace:

When you implement an airtight Social Media Policy, and all employees are aware of what can and cannot be posted, this can actually help you to increase the awareness of your products and services to prospects. This can also lead to meaningful conversations being carried out on the chat platforms, and this in turn can ultimately drive revenue and help you to achieve a greater Return On Investment (ROI) on your marketing efforts. The use of Social Media sites for marketing and advertising to connect with customers is only going to proliferate to much greater levels in the future. For example, at the present time, it is estimated that some 47% of American workers use some kind of Social Media platform to have a dialogue with a prospect or customer.

(SOURCE: 6).

4) It will help to mitigate the probability of a Cyberattack:

Those individuals that make up the security team in the IT Department have enough to do as it is with trying to combat the daily threats that are occurring, trying to filter through thousands of false positive alerts and warnings, and trying to analyze intelligence feeds to predict the future threat landscape. The last thing that they need to be worried about is trying to thwart off a new threat vector that got through because of an improperly used Social Media Site. By constantly reminding employees of the importance of maintaining good levels of “Social Media Hygiene” and the consequences for not doing so, this should help reduce the probability of a Cyberattack being launched through an employer owned Social Media site, as well as Personal Identifiable Information (PII) from being stolen.

5) It will protect the company from potential lawsuits:

By detailing exactly what can and cannot be posted on a company Social Media site will actually prevent you from being financially responsible in a legal filing. For example, if an employee files a lawsuit stating that they were being improperly treated with regard to Social Media usage during work hours, and if you can prove to a court of law that the employee was continually reminded of what was permissible to post, the chances are much greater that the lawsuit will be thrown out. Also, in today's Cybersecurity world, many of the entities in Corporate America are now starting to realize the importance of having a Cybersecurity Insurance Policy in case they are hit with a security breach. When you file a claim, your insurance company will carefully scrutinize every aspect of your security operations, especially when it comes to Social Media usage. By proving that you have an airtight policy, this will also enhance the probability of getting a 100% payout on the claim that was filed.

The Components of a Social Media Policy

Just like a Security Policy, creating a Social Media Policy is very often subjective, as a lot of it depends upon how your business uses the various Social Media platforms that are available out there. Therefore, a lot of it will depend on the type of content that is posted, how often, if you allow for interactions between employees and prospects/customers, whom have access to it, the privacy setting thresholds that are applied, etc.

The following components are considered to be what all social media policies should contain, at a minimal level. They are as follows:

- All employees must acknowledge that they have been educated about the use of company and personal Social Media sites during work hours, and this is done by having them sign an official document attesting to this fact.

- When posting any kind of content, all employees must follow the organization's strict rules of conduct when it comes to online behavior;

- Under no circumstances, will any employee reveal any confidential information or data about any customer, or any company trade secrets, whether knowingly or not. The consequences could include up to an immediate termination.

- Before any employee can post content on a company owned Social Media site, they must first show it to their immediate manager and get prior approval. If this is not strictly followed, then the employee will be held personally liable for any negative consequences that could precipitate from it.

- Employees can access their personal Social Media sites on company property only when they are considered to be "off the clock", such as during the lunch hour, or during designated break times. Access to personal sites can only be gained by using their own device, and not through company issued ones.

- All employees should not expect any privacy rights whatsoever when they are accessing and posting Social Media sites, whether it is a company or personal account, during work hours.

- Any form of interaction or communication that an employee engages in with a prospect and/or existing customer and vice versa is the sole property of the company.

- Accessing any company owned Social Media platform is only permissible through company owned and issued devices to the employees. Under no circumstances whatsoever, can a company owned Social Media platform be accessed through a personal device. For that matter, the access of company owned Social Media sites can only be done on the physical premises of the company, or the through the remote access policies that have been set forth in the Security Policies. These sites cannot be accessed through any public and unencrypted Wi-Fi hotspots, under any circumstance.

- It is important to keep in mind that Social Media Platforms do not refer simply refer to the specific brand names of Twitter, Facebook, Linked In, You Tube, Instagram, Pinterest, etc. This also extends to other areas where company related content is posted and is available for public viewing that is external to the company. This even includes company blog sites, podcasting sites, online forums (and other related discussion boards, etc.). The same Social Media Policies are totally and completely applicable to these non-branded sites and platforms as well.

- Whenever an employee posts content of any type or kind of any branded or non-branded Social Media Platform, he or she must include a disclaimer that the views that are posted are strictly their own, and not the entire organization's views.

- All Social Media Platform rules and regulations are also applied when posting any kind or type of content in dealings with external third parties that are affiliated with the company, which includes the likes of suppliers, distributors, transport entities, and other forms of outsourced entities.

- Under no circumstances will access to Social Media Platforms, both company or personally owned, shall interfere with the daily job functions that the employees are expected to perform, and the deadlines they are tasked with.

- Under no circumstances whatsoever, can any type or kind of copyrighted material be posted on company branded and non-branded Social Media Platforms. If there is any doubt to this, the employee must then present and defer this matter to his or her immediate manager, whom in turn, will get feedback from the company legal team before proceeding any further.

- If an employee has witnessed the act of another employee violating any terms or conditions of the Social Media Policy, he or she must then contact their immediate manager as well as the Human Resources (HR) Department.

- All employees posting content on company branded and non-branded Social Media Platforms, must under all circumstances, exercise good judgment so that no local, state, and federal laws are violated.

It is also important to keep in mind that other key areas of an effective Social Media Policy must be addressed as well, but these are totally dependent upon your company's requirements and resources. These are as follows:

1) Decide who will speak on behalf and post content about company related matters;
2) Have an action plan implemented in case a piece of content that has been posted on a Social Media Platform is causing grave conflict, such as that of misunderstood communications between employees and prospects/customers, and even vice versa.

3) A strategic plan as to how to respond to and resolve any legal action that has been filed against the company as a result of a Social Media Platform posting;

4) Have a crisis plan ready–for example, if somebody posts something about an employee's action during off-work hours, who and how will this be dealt with?

5) Who will be responsible for reviewing the Social Media Policy as it relates to Federal Labor Laws?

6) Which employees will be granted exclusive access to the company owned Social Media Platforms, and those that can create new accounts.

7) Which department of the company will be held responsible and accountable for making sure that the Social Media Policy is updated on a regular basis, as well as the enforcement of it.

Conclusions – Examples of Social Media Policies That You Can Use S

One of the best ways in which to craft a Social Media Policy is to take a look at how other business have created theirs. Here are some examples of them that have been implemented by the Fortune 500:

For Yahoo, click here.

For Coca Cola, click here.

For General Motors, click here.

Finally, after you developed your Social Media Policy, it is always best to have your in-house legal team review it first before implementing it. Remember, not only do you have to protect your company's rights, but your employees also have rights that need to be protected as well.

Sources

1) https://blog.hootsuite.com/social-media-security-for-business/
2) https://www.phoenix.edu/news/releases/2016/04/uopx-social-media-hacking.html
3) https://www.emarketer.com/content/users-have-little-faith-in-social-networks-privacy-protections
4) https://searchcompliance.techtarget.com/definition/social-media-policy
5) https://www.pewresearch.org/internet/2016/06/22/social-media-and-the-workplace/
6) http://www.adweek.com/digital/social-media-job-screening/
7) https://www.business2community.com/cybersecurity/7-social-media-security-issues-business-faces-02024378
8) https://www.smperth.com/news/social-media-and-cyber-security-risks-in-2019/

9) https://www.thesecurityawarenesscompany.com/2017/06/06/cyber-security-risks-social-media-5-ways-users-vulnerable/

10) http://www.brandquarterly.com/social-media-policy-important-brand

11) https://www.hrduo.com/blog/3-reasons-why-your-company-should-have-a-social-media-policy

12) http://thesocialworkplace.com/2011/04/elements-of-an-effective-social-media-policy/

13) https://sproutsocial.com/insights/social-media-policy/

14) https://blog.gaggleamp.com/blog/blog/what-should-a-good-social-media-policy-include

15) https://www.powerdms.com/blog/six-elements-good-social-media-policy/

16) https://www.ragan.com/6-terrific-examples-of-social-media-policies-for-employees/