Security threats through social media information technology essay

Technology, Information Technology

The analysis has given us an insight about the strategies and controls that can be used to overcome the challenges and mitigate the risks associated with social media. Enterprises and users using social media must clearly understand both the benefits and risks of engagement in social media activities. For most organizations, social media offers significant opportunities to accelerate their ability to launch new brands, incrementally strengthen customer relationships and drive revenues from existing and new customers. However there are numerous security risks that accompany these benefits. The report attempts to focus on identifying these risks, their sources, mitigation techniques and the guidelines to provide assurance against the same.

INTRODUCTION

Definition

The term Social Media has come into existence fairly recently. Social Media refers to online interaction that allows for user-generated content in the form of text audio, video, images etc. to be published in a highly scalable manner for general public consumption, often involving interactive dialogue with others. The communications is Social Media tend to be highly dynamic and interactive, yet personal in nature.

History

Although a recent phenomenon, the core capabilities of social media can be drawn from a long lineage of electronic communication. The trend of using electronic media to communicate broadly did not begin with MySpace and Facebook or even predecessors like Friendster. In fact, the foundation of the

Arpanet, the pioneering technology for the modern Internet, was largely driven by the need to communicate between various government and university researchers. Ever since the first email was sent in 1971, email has always been a common form of social media, especially when it goes beyond one-to-one communication. From email evolved list services (listservs) and more recently came the use of wikis, blogs and other online communication that equal the functionality found in modern forms of social media such as Facebook and Twitter. In fact Facebook and Twitter too are derivatives of blogging – known as micro blogging. Therefore, the emergence of social media cannot be considered unique or isolated, but instead a result of constant evolution of online communications - but with distinct considerations due to being used in an exceptionally broad setting. The requirements for security controls may also not be unique, but applying them can be challenging given the magnitude and scale at which these technologies are deployed. Through this paper, we attempt to shed light on the various types of social media, business benefits that social media affords to organizations, the numerous security risks associated with social media, the sources of these risks and proposed guidelines to provide reasonable assurance against the risks of social media.

TYPES OF SOCIAL MEDIA

There are predominantly nine types of commonly used social media. Wikis: It is the most widely used website that allows users to add, modify or delete contents via web browser. Blogs: These are the online forums that allow members to hold conversations by posting messages. or write-ups on any particular topic. Micro-blogs: Forum that focuses on short updates that are pushed out to anyone subscribed to receive the updates. Social Networking: This is a form of service that allows people with similar interests to connect on common forum. Videos: This forum allows individual to share videos on any topics relating to their field of interest. e. g: Youtube. Discussion forums: These are the online forums, which allows individuals to share their ideas and thoughts pertaining to a topic. Podcasts: It is forum where audio; video, PDF or ePUB files are uploaded or downloaded by the users. Photo Sharing: It is service provided many websites and applications where users upload and transfer their digital photos. News Feed: This allows people to post various news items or links to outside articles and then allows its users to comment and vote on the items.

BENEFITS OF SOCIAL MEDIA TO THE BUSINESS ENTERPRISE

The social media revolution has completely transformed the business communications landscape and the way in which businesses reach out to new markets and interact with customers. It has opened up new vistas, and brought with it an abundance of avenues for businesses to augment customer satisfaction, sales, brand recognition, search engine optimization (SEO), web traffic, and revenue. Additionally, rapid insight and feedback from customers afforded by the social media allows the organizations to evaluate consumer opinion in order to improve products, perception and customer service. Through social media, organizations are able to monitor not only the market and their customers, but also their competition. This enables the engaged organizations to be on top of any changes required or adjustments made to strategies, products or services. Sites such as LinkedIn and Plaxo have also the ability of organizations to search for and communicate with potential employees. Below are the responses of respondents of a survey conducted to find out the top three benefits of social media to their respective organizations:

Figure 1

Therefore due to its tremendously large and instantaneous reach, while still being easy to use and measure, social media is becoming a commanding force in the way businesses reach out to, invite and engage their customers, employees and other stakeholders. Enterprises that have aggressively embraced social media as part of their strategy have been found to be much more financially successful than those who don't. However, " Social media isn't inexpensive, it's just a different expensive." (Charlene Li)

THREATS & VULNERABILITIES, RISKS AND RISK MITIGATION RECOMMENDATIONS

Threats of social media and risks arising through its use come in two ways – through corporate social media presence and employees' social media presence.

Risks of a Corporate Social Media Presence

Threat #1: The most common threat or vulnerability from social media presence is the the organizational network being attacked by viruses and malware. This leads to the risks of data leakage and theft, wherein the attacker gains access to the organization's valuable information resource thereby putting at stake the confidentiality and integrity of the information.

It can also lead to ‘ owned’ systems or zombies, in which the attacker obtains full control of the organization’s system. System downtime can also arise through such attacks leading to compromising the availability of information. In order to mitigate the above risks, the organization must ensure that the latest antivirus and antimalware controls are installed on all systems and are updated daily. The use of content filtering technology must be considered to limit or restrict access to social media sites. Appropriate controls on mobile devices like smartphones must be installed. It is also important to establish and frequently update policies and standards, and to develop and conduct awareness campaigns and training to educate employees regarding the risks related to the use of social media sites. Threat #2: Another threat arising through corporate social media presence is hijacking of the corporate website leading to exposure of the enterprise and customersThere are various risks associated with a hijacked website. The organization may have to face backlash from customers and sometimes even adverse legal actions. Exposure of sensitive or confidential customer information, damage to the organization’s reputation and targeted phishing attacks on customers or employees can become prevalent. Risk mitigation techniques that can be employed to prevent the above risks from surfacing include engaging a brand protection agency that can probe the Internet and look out for misuse of the enterprise brand, providing periodic information and updates to customers imparting awareness of potential fraud and to establish clear guidelines relating to what information must be posted as part of the enterprise social media presence. Threat #3: Undefined or unclear content rights to information posted to social media sites. Such ambiguity of content rights can lead to the enterprise losing control or legal rights over information posted to social media sites. In order to mitigate this risk, the legal and communications teams of the organization must carefully review user agreements for each of the social media sites being considered. Clear policies must be established that dictate to employees and customers what information should be posted as part of the enterprise social media presence. Ensuring that there is a capability to capture and log all communications can also prove very beneficial. Threat #4: Making a move toward a digital business model can increase customer service expectations. Customer satisfaction may become directly proportional with the responsiveness received in the social media arena, causing potential reputational damage for the enterprise in case of delayed or inconsistent responses. It can also lead to customer retention issues. The organization can mitigate these risks by making sure that there is adequate staffing to handle the huge amounts of traffic that can be created by a social media presence. It can also help to create notices providing clear windows for customer response. Threat #5: The perceived risk of mismanagement of electronic communications, which are often administered by regulations and electronic audits. Electronic communications are often governed by numerous regulations, and mismanaging the media for electronic communications can lead to adverse litigations, regulatory sanctions and fines. It is essential to establish appropriate policies and processes, and install the necessary technologies to ensure that all communications through social media that might be impacted by legal requirements are tracked regularly and archived appropriately. However, it may not always be feasible to maintain an archive, depending on the social media site being used. For instance, communications through video sites like YouTube can take up immense space for archiving and drastically increase overheads. Moreover, social media nowadays is a major contributor to the ‘ big data’ being produced and stored with each passing second, so archiving all that data can be extremely cumbersome and impractical for the organization.

Risks of Employee Personal Use of Social Media

There are a number of risks emanating through employees’ personal use of social media as well, which makes it necessary for the organization to keep an eye on the social media activities of its employees. Threat #1: Work-related information being communicated through personal accounts. Employees communicating material work-related information, intentionally or unintentionally, through their social media accounts may put the organization at the risk of privacy violations or even loss of competitive advantage, especially when that information was not meant to be disclosed publicly. In case of negative remarks about the work place, there can also be reputational damage to the company. In order to mitigate the above risks, it is essential to work closely with the human resources (HR) department for establishing new policies or ensuring that existing policies address all issues related to employee postings of work-related information. The HR department must design awareness campaigns and training programs to reinforce these policies. Threat #2: Employees posting pictures or other information which links them to the enterprise. Merely casual posts by employees that link them to the enterprise may potentially cause damage to the reputation and brand of the enterprise. The HR department must develop policies that clearly specify how employees may use enterprise-related videos, images or any other media in their online presence. Any enterprise assets and intellectual property should not be allowed to be used by employees in their online activities, and this message must be clearly put across to all in the organization. Threat #3: Excessive use of social media in the workplace by employees. Excessive social media activity in the workplace can give rise overloading of organizational networks. It can also lead to increased risk of exposure to malware and viruses. Productivity loss of employees is also a common consequence. Limiting network throughput to social media sites or content filtering can help manage accessibility to social media sites at the workplace. Threat #4: Employees accessing social media through enterprise-supplied mobile devices such as smartphones and personal digital assistants (PDAs)Accessing social media via enterprise-supplied mobile devices can lead to infection of the mobile devices, circumvention of enterprise controls, data theft and data leakage from the mobile devices. To mitigate the above risks, all enterprise smartphones communication must be routed through the corporate network filtering technology in order to limit or restrict access to social media sites. The appropriate controls must be installed and regularly updated on mobile devices just as done on office computers. Establishing or updating policies and standards pertaining to the use of mobile devices is important, and must be followed up with designing and conducting awareness campaigns and training to inform employees of the same.

GUIDELINES FOR ASSURANCE

As much as it is the responsibility of enterprises to develop appropriate strategies and place robust controls for managing their social media presence, it is the duty of assurance professionals within the organization to monitor and validate these controls to make sure that they are, and continue to remain, effective and that adherence to these controls is honored and is measurable. The following elements can provide a good foundation for assurance professionals to deliver the assurance that risks are being managed properly:

Governance and Strategy

It is important to first conduct as a risk assessment to map the risks presented by the use of social media. This assessment must evaluate the specific social media sites to be used and the business processes planned for leveraging social media. Whenever there is any substantive change in the social media resources or they're use, the risk assessment must be revisited. The assurance professional must also verify if there is an established policy and standards to support it which address the use of social media – both business and personal, and these policies and standards must be updated regularly. There are four main areas that policies governing social media use must address: Personal use of social media by employees in the workplacePersonal use of social media by employees outside the workplaceUse of social media by employees for business purposes, through personally owned devicesMonitoring and follow-up processes required for brand protection

People

The assurance professional must ensure that effective training has been imparted to all users and that regular awareness communication regarding risks and policies is made with all users and customers. Also it must be assessed how clearly the users understand what is appropriate or inappropriate in terms of social media usage and how they can protect themselves and the enterprise from the risks posed by social media. Customers too must be educated regarding what appropriate use of the channel is considered to be, and what kind of information they may or may not share.

Processes

It is imperative to review the business processes which utilize social media in order to make sure they are aligned with the policies and standards of the organization. This is because unless and until business processes are in line with the social media policies, there cannot be reasonable assurance that they would not place the enterprise at risk through the exposure of sensitive information or otherwise. And change controls must also be placed so that any additions or changes to processes that leverage social media are lined up with the social media policy prior to their implementation.

Technology

The assurance professional must examine if the IT department of the enterprise have a strategy and the capabilities to support it, to manage technical risks posed by social media. In terms of technical risks posed by social media, a vast majority lies in the use of malicious e-mails and standard web sites. The IT department must be well-equipped to place both network-based and host-based controls to mitigate risks posed by malware. Appropriate controls may include data leak prevention products, secure browser settings, download restrictions, content filtering and monitoring, and antimalware and antivirus applications. Any infection that does manage to get through can be countered through sound incident response plans (IRPs). All technical processes and controls must have been designed in a way as to adequately support the policies and standards pertaining to social media, and must be verified and found to be present and functioning as expected. Or in case of future plans, there must be clear timelines and the required budget in order to reach a particular capability. Also, the enterprise must have an established process to counter the risk of fraudulent or unauthorized use of its brand on the social media sites that could negatively impact the enterprise. This risk exists even if the enterprise does not actively use social media. Even though probing for such material can be cumbersome, it is essential for the enterprise to have a strategy against this risk. A number of third party vendors offer this service, which this is usually the best alternative for enterprises that consider such monitoring to be necessary.

CONCLUSION

Although, social media has witnessed a massive increase in communication and interaction in past decade, they also have raised concerns regarding privacy and security. Both, organization and users have to be more prompt in capitalizing on benefits and dealing with the threats of social media. Social media provides several opportunities for users and organizations to gain numerous benefits. This includes better social interaction, brand publicity, e-business, e-education etc. The benefits of using social media comes with its pitfalls i. e. its potential risks and costs associated with dealing with those risks. In this paper we, have discussed various forms of risks, threats associated with social media and the methods to mitigate those threats. Training and awareness programs play a pivotal role in eliminating the risks caused by improper use of social media. Also, with the right strategies, policies, and guidance in place, it can be an extremely effective communication tool with far-reaching benefits across demographics, organizational groups, and individual communities.

REFERENCES

BITS, A Division of the Financial Services Roundtable. " Social Media Risks and Mitigation." (2011): 1-71. Print. Baer, Jay. " 18 Social Media Quotes." Convince and Convert: Social Media Strategy and Content Marketing Strategy — Social Media Strategy Social Media Consulting Content Marketing Strategy Content Marketing Consulting. Web. Bullas, Jeff. " 12 Major Business Benefits Of The Social Media Revolution | Jeffbullas's Blog." Social Media Marketing and Blogging. Jeffbullas. com, WebDinerman, B. (2011). " Social Networking and Security Risks." 8. Messmer, E. (2012). " Social media brings business, but complicates security." 29(10): 1, 32. ISACA. " Social Media: Business Benefits and Security, Governance and Assurance Perspectives." ISACA (2010): n. page. Print. Chatzitheodosiou, G. M. (May 2012). " Security Information and Event Management - " ID, Adapt, Secure": An applicable approach for modern Social Networking Platforms."

Proposal for AFCEA Student Conference. data, d. " Towards 'Social' Security." Michael E. Whitman, H. J. M. (2011). " Principles of Information Security." (Fourth). qualman, e. (2013). " socialnomics - how social media transforms the way we live and do business." (second). Ponemon Institute LLC. " Global Survey on Social Media Risks Survey of IT & IT Security Practitioners." (2011): Print