Auditing Social Media

New inventions are created every day. Some fail and go nowhere, while others revolutionize the world and change the way people live. Most would argue the Internet is among the inventions that did just that. The Internet has transformed the way people communicate like nothing before, which is largely the reason for its success and sustainability. It is a mechanism for information sharing and a means to collaborate and interact with individuals without regard for physical location. In the 1990s, the World Wide Web became popular, and it was then that many organizations made the business decision to have a presence on the Internet by creating their own websites. It was seen as a way to increase a company's competitive advantage. Before then, the Internet was limited to education, research and the government.

As early as 1994, social media was born. However, it was not until 2006 that social media became hugely popular. This popularity is not only among individuals.

Paul Phillips, CISA, CISM
Is technical research manager at ISACA®. Phillips has extensive auditing, management (people and projects) and teaching expertise. His industry-sector experience includes pharmaceuticals, insurance, manufacturing, business services and real estate. Phillips is an instructor for multiple higher-learning institutions, including Aurora University and Lewis University (Illinois, USA). He is founder of a not-for-profit organization aimed at helping youth develop skills for academic and vocational success.

Today, businesses are getting in the game because there is a clear competitive advantage to using social media. The concern now is if the risk and the associated safeguards are understood.

As of December 2015, Facebook had surpassed 1.5 billion monthly active users. In March 2016, Twitter reported 320 million monthly active users. Instagram's September 2015 figures indicated 400 million users and more monthly active advertisers (200,000 vs. 130,000) than Twitter.[1] With the popularity of social media, it is no wonder that many companies have decided to take advantage of this technology. Some have even stated that social media is the most powerful tool for marketing in today's environment. As with the Internet, the business community has once again seized the opportunity this technology brings.

Benefits and Risks

There are many reasons why businesses can benefit from social media: They can gain valuable customer insights, increase brand awareness and loyalty, run targeted ads with real-time results, generate higher converting leads, provide rich customer experiences, increase website traffic and search ranking, find out what competitors are doing, share content faster and easier, geotarget content, and build relationships.[2]

However, what is not so popular and well known is the risk of both the Internet and social media to the enterprise. The potential for the risk of hackers accessing the company's information assets in an effort to steal or damage these resources automatically increases each time a company makes the decision to connect their corporate network to the Internet.

For most enterprises, being connected to the world's largest network and the resulting increase in the organization's visibility are seen as being worth the risk; the same applies to social media. Having a presence on social media and allowing access to such sites on the company's computer resources are seen as being well worth the risk.

Risk Mitigation

Because of this social media use, most enterprises have implemented multiple safeguards to mitigate this risk. Among the types of risk to which social media can expose the enterprise are reputational damage, information leakage, regulatory noncompliance and loss of intellectual property.

Access to the company's social media site should be granted based upon an approved request. Otherwise, it should be blocked through existing firewall and filtering technology. Once approved access is granted, managing content can be challenging and should become a part of the security monitoring procedures. Other controls that should be in place are acceptable use policies, a security awareness program, training and education, and other electronic controlling mechanisms, e.g., intrusion prevention and detection systems.

Losses to organizations due to computer attacks, such as denial of service, phishing and password attacks, are all too common in today's world. It should be noted that the root cause for some of these attacks is connectivity to the Internet and the decision by enterprises to allow access to various social media sites. Because of this risk to organizations, it is important that they include it as part of their overall audit plan.

When the average businessperson thinks of auditing, he/she thinks in terms of financial statements, and such audits are indeed important. One of the main objectives of a financial audit is to perform an examination to determine whether there are effective controls in place to protect the assets of the organization from the risk of theft and loss.

An IT audit has the same objective; however, the controls under review are technical in nature and the assets are not just financial, but include information and the company's reputation and intellectual property.

Performing the Audit

When performing an audit of social media, the auditor should consider whether the enterprise has a policy in place that clearly denotes what is acceptable and unacceptable use of social media. The auditor should also ascertain whether this policy is in alignment with the overall strategic plan of the organization. The organization should have detailed procedures or a training plan explaining how to comply with the policy. This training should be accessible and possibly mandatory to employees, depending on their role in the organization. The auditor should also obtain an inventory of the enterprise presence on all social media sites and determine if there is monitoring for each instance in place. The following are a few key steps in performing a social media audit:[3]

> **When performing an audit of social media, the auditor should consider whether the enterprise has a policy in place that clearly denotes what is acceptable and unacceptable use of social media.**

- Determine if a risk assessment to identify inherent risk associated with this form of technology was performed.

- Determine if social media information has been included in the data classification process.

- Determine if there is a policy in place explaining the acceptable and unacceptable use of social media on the enterprise's electronic resources.

- Determine if social media access is covered in the access management procedures.

- Determine if antivirus software is implemented with the appropriate settings to mitigate risk associated with social media.

Conclusion

While social media is very popular and obviously here to stay, there is a dark side. Many enterprises have made it a part of their marketing tool kit and are seeing benefits. However, an audit of this technology should also be seen by management as a valuable tool that ultimately helps protect the enterprise by reporting on the level of effectiveness of the safeguards put in place in response to the associated risk. When enterprises utilize the tools at their disposal in an effective manner, they are able to enjoy the rewards and mitigate risk at the same time.

Endnotes

1   Social Times, "Here's How Many People Are on Facebook, Instagram, Twitter and Other Big Social Networks," *Adweek.com*, 4 April 2016, *www.adweek.com/socialtimes/heres-how-many-people-are-on-facebook-instagram-twitter-other-big-social-networks/637205*
2   Copp, E.; "10 Benefits of Social Media for Business," Hootsuite Blog, 17 August 2016, *https://blog.hootsuite.com/social-media-for-business/*
3   ISACA®, see Social Media Audit/Assurance Program, USA, 2011, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Social-Media-Audit-Assurance-Program.aspx*