Social Media Rewards and Risk

Disponible également en français
www.isaca.org/currentissue

Social media is a powerful tool that gives organizations the ability to expand their brand value; it can also tarnish a brand overnight. There are more than 18 social media platforms globally that have started to grow and have an enterprise-level following, and this is only the beginning. Given the visibility, risk, and real-time monitoring and response required to effectively manage social media channels, companies must establish extensive protocols for use by their organization in order to engage with external channels. Companies representing themselves externally should engage the appropriate and authorized spokespersons and executives designated by their communications department in order to speak to, initiate, provide and/or post information within the social media space. While there are several key risk factors to be addressed relative to social media, there are many rewards as well. Some of the most advanced topics and benefits include (**figure 1**):

- **Connecting with customers**—The ability to engage with customers is the most critical aspect of social media. Developing a brand and promoting it through various channels of social media can create further brand value and awareness.
- **Marketing intelligence**—Social media marketing gives the organization the ability to monitor the brand and listen to what the public is saying in the social media space. The insight is the reward the organization reaps by playing a larger role in social media, which can be invaluable. The organization can enhance its marketing, business development efforts and other valuable venues to further its ability to be competitive.
- **Pulse on brand reputation**—Keeping the pulse of the organization's social media reputation and metrics is critical to staying ahead of the brand's recognition and signs of reputational risk.

As for the risk (**figure 2**), some of the most common ones include:

- **Reputational risk**—Damage to an organization's reputation stemming from a social media mishap can bring the organization to its knees, whether it is the chief executive officer (CEO) stating something controversial on his/her Twitter account or an organization-bashing employee video that goes viral. According to a leading publisher, "A reputational crisis can wipe tens of millions of pounds from a company's value, and this risk has increased because the rise of online and social media means crises are now less predictable and can happen faster."[1]
- **Data security breach**—According to research from Forrester:

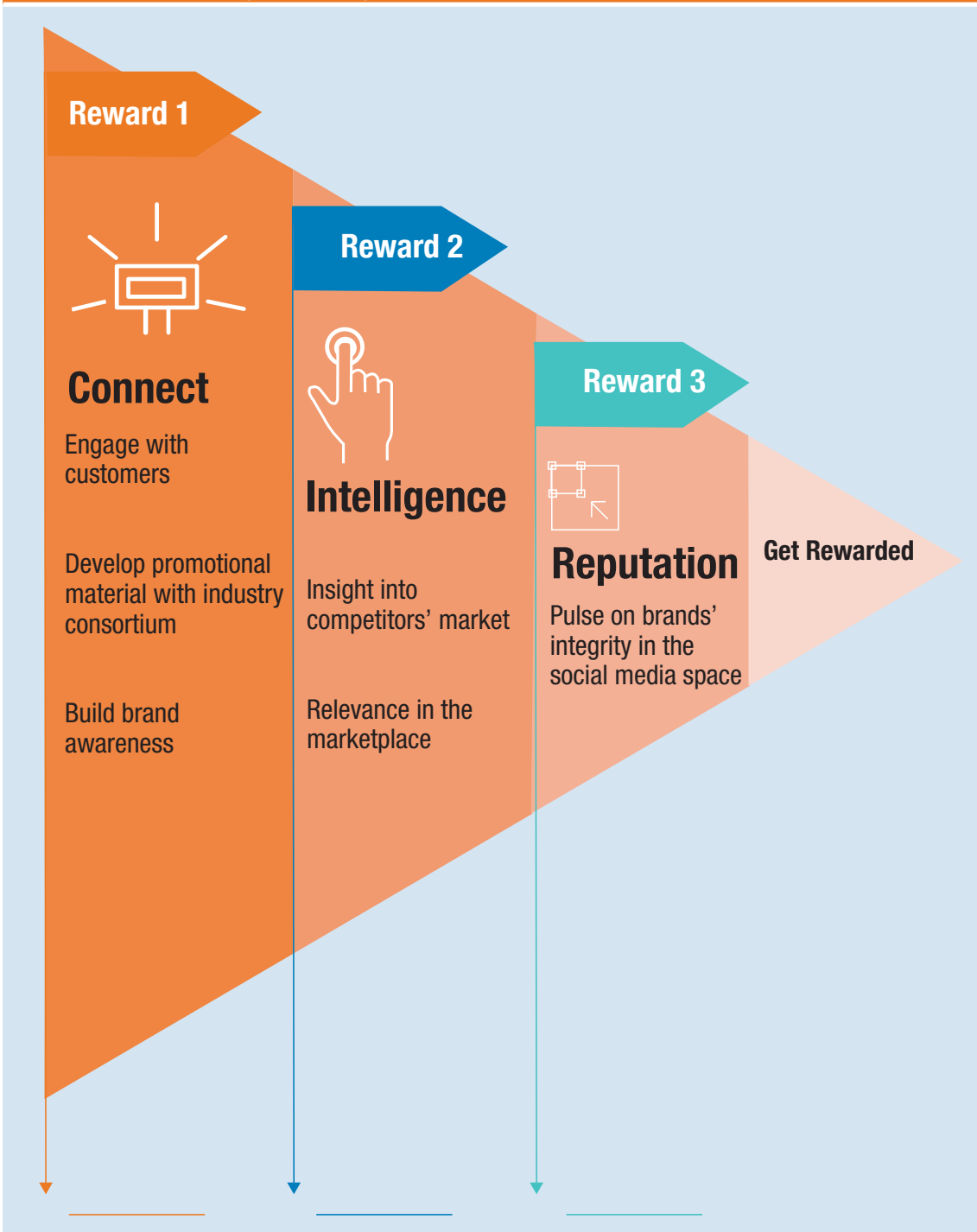
  From reconnaissance to brand hijacking and threat coordination, cyber criminals have been using social media to boost the effectiveness of their attacks for years. It's clear that social media risk isn't solely about brand and reputation damage but is a sinister cybersecurity threat that can lead to major data breaches, numerous compliance issues, and large amounts of lost revenue due to fraud and counterfeit sales, along with a slew of other risks.[2]
- **Social engineering**—Employees in almost all organizations are savvy, and many have a social media presence on major sites such as Facebook, LinkedIn, Quora and Twitter. Each platform has

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2sUGrw7

Mohammed J. Khan, CISA, CRISC, CIPM
Is a global audit manager at Baxter International, a global medical device and health care company. He has more than 12 years of experience focused on providing privacy, security and information governance. Most recently, he has focused specifically on medical device cyber security, global privacy frameworks, and helping his organization with strategic, cost-effective initiatives in the audit and compliance space. Khan previously worked for a leading consultancy firm as an assurance and advisory professional, and prior to that, he worked as a global enterprise resource planning and business intelligence professional at a leading technology firm. Khan has helped develop and author several publications and has presented at industry conference events focusing on privacy and cyber security.

Figure 1—Organizational Benefits of Social Media



Source: M. Khan. Reprinted with permission.

the potential to provide a hacker several key data points about employees, which can enable use of the data to hack the employee account at the enterprise layer by spoofing and launching a social engineering attack on the company. Due to the multitude of options of going through social media accounts with exposed data, attackers can gather these data to further their advances in terms of hacking into accounts.

- **Compliance or regulatory violations**—The growing number of privacy changes and regulations globally is impacting how customer data are utilized in the social media space. There are four key areas with which to be concerned:
  – Privacy
  – Content ownership
  – Intellectual property (IP) infringement
  – Unauthorized activities

> **"Employees who access social media websites can act as brand ambassadors; on the other hand, their activity may leave an open door for viruses and malware to enter into the network."**

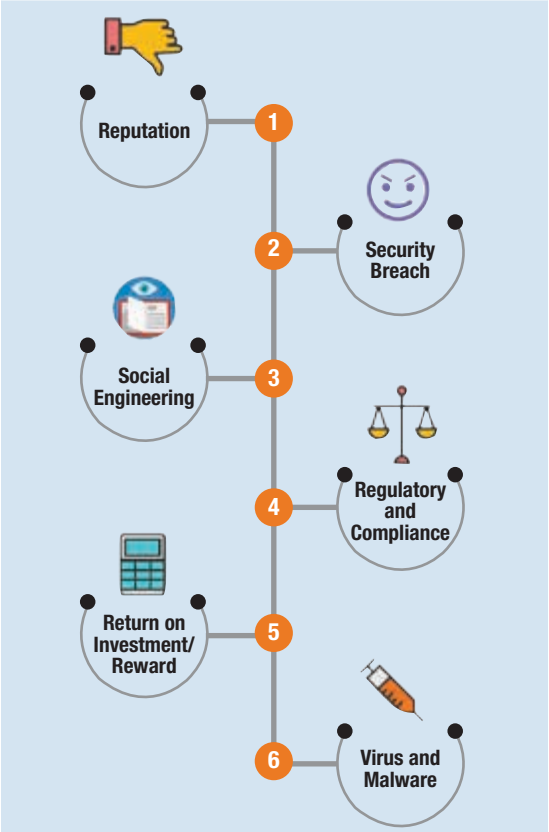
- **Compliance to changing the regulatory climate**[3]—These regulatory changes require the organization to adapt its strategy if it wishes to comply on a global basis. This approach, while necessary for an organization that uses social media regularly, may result in the organization's increased visibility with authorities.

  Some industries may shy away from this situation in light of audits that occur due to being in the social media space so frequently.

- **Return on investment**—The benefit the organization gains from being present in the social media space is hard to calculate and very subjective. The risk over reward, therefore, cannot be calculated without proper assurance, which leaves the decision to enter the social media space questionable for some industries.

- **Phishing**—One of the popular techniques used by criminals is to get unknowing individuals to disclose personal information while posing

Figure 2—Risk Factors for Social Media



Source: M. Khan. Reprinted with permission.

Enjoying this article?

- **Learn more about, discuss and collaborate on risk management in the Knowledge Center.** *www.isaca.org/risk-management*

as a fictitious representative of a legitimate professional or company. This, primarily, is the key driver for collecting personal data for financial gain to individuals or organizations. Due to the lack of awareness about the phishing techniques used by hackers, employees fall victim to email, phone call and website phishing schemes, resulting in exposure to enterprise-level risk.

- **Viruses and malware**—Hackers' ability to penetrate the organization's network via unsafe social media websites and accounts opens a new threat vector. On one hand, employees who access social media websites can act as brand ambassadors; on the other hand, their activity may leave an open door for viruses and malware to enter into the network. According to security experts, "A majority of current attacks simply use the social platforms as a delivery mechanism, and have been modeled after the older Koobface malware."[4]

Preventing Social Media Risk

Some organizations struggle to develop the best solution to manage risk around social media. The first question to ask is who, in fact, owns the social media platforms for the organization and, more importantly, the overall governance of the social media of employees. Social media impacts all departments of the organization, and each department, whether it is IT, finance, marketing or human resources (HR), has a different perspective of how social media can or will be utilized by the department on behalf of the organization. There is no prescribed rulebook for eliminating social media risk to an enterprise; however, some key areas to consider for preventing social media risk are:

- **Guidelines**—As general best practice, a high-level overall policy should be rolled out to guide the use of social media by all employees of the organization and any third party acting on behalf of the organization. The guidelines should highlight key components including:
  - **Scope**—Defining the overall scope of the policy guidelines that is set forth by the enterprise for its employees
  - **Purpose**—Definition of the purpose of the guidelines for the organization, specifically, how social media activity on behalf of the organization will take place and what sort of information is relevant to share via that activity

> **"A robust social media crisis and communication plan must be developed in the event that a crisis occurs."**

  - **Goals**—Clear definition of the overall outcome that is to be achieved from the social media presence for the organization and how the social media platform will get the organization there
  - **Ownership guidelines**—General guidelines for the creation and maintenance of all social media sites for the organization

  - **Contributor guidelines—**General guidelines and principles directing contributors to the social media sites
  - **Approved social media platforms—**Expectation for departments assessing social media solutions outside of the company to demonstrate how the social media presence will contribute to achievement of the overall goal and, more importantly, the platform's degree of utilization and security

- **Training and awareness**—It is key for the organization to embody the proper use of social media etiquette as part of the onboarding training of all employees, especially in roles such as marketing, HR and IT—departments that will most likely be representing the organization as part of their ongoing job functions. Embedding the behaviors and instilling the right concepts of social media norms that align with the organizational policies and processes will help in the long run as more and more employees participate on social media and represent their organization and its products and interests.
- **Social media crisis and communication plan**—A robust social media crisis and communication plan must be developed in the event that a crisis occurs. There has to be a single point of contact, usually the communications team, for all communication with the media and stakeholders. Key department personnel have to be involved, especially if there is a matter that applies to that specific department.

It is critical to practice the plan in terms of performing the scripted tasks required for smooth control of the social media crisis that is bound to happen to any organization as its social media presence increases over time. This requires significant amounts of collaboration and communication across key departments and personnel at all times.

Conclusion

Organizations that plan to increase or decrease their presence on social media would be well advised to exercise awareness and vigilance. Different industries may experience various benefits and disadvantages to jumping on the social media bandwagon. Organizations planning to engage on social media platforms must have a clearly defined policy and communication plan in place. Proper considerations should be made for good governance, a communication plan in the event of a breach, a social media policy and monitoring tools, which are all important for enterprise-level social media risk mitigation.

Deciding which social media channels to use and performing due diligence and evolutionary management of the social media space the organization enters are critical. The first step is to understand the benefits and the disadvantages while keeping in mind the basic steps that can be taken to mitigate risk.

Endnotes

1 Spanier, G.; "Reputational Risk in the Social Media Age," *Raconteur*, 11 June 2015, *https://www.raconteur.net/business/reputational-risk-in-the-social-media-age*
2 Hayes, N.; "Why Social Media Sites Are the New Cyber Weapons of Choice," *DarkReading*, 6 September 2016, *www.darkreading.com/attacks-breaches/why-social-media-sites-are-the-new-cyber-weapons-of-choice/a/d-id/1326802*
3 McNickle, M.; "5 Keys to the Legal Issues of Social Media in Healthcare," *Healthcare IT News*, 2 July 2012, *www.healthcareitnews.com/news/5-keys-legal-issues-social-media*
4 McAfee, "How Cybercriminals Target Social Media Accounts," *https://www.mcafee.com/us/security-awareness/articles/how-cybercriminals-target-social-media-accounts.aspx*