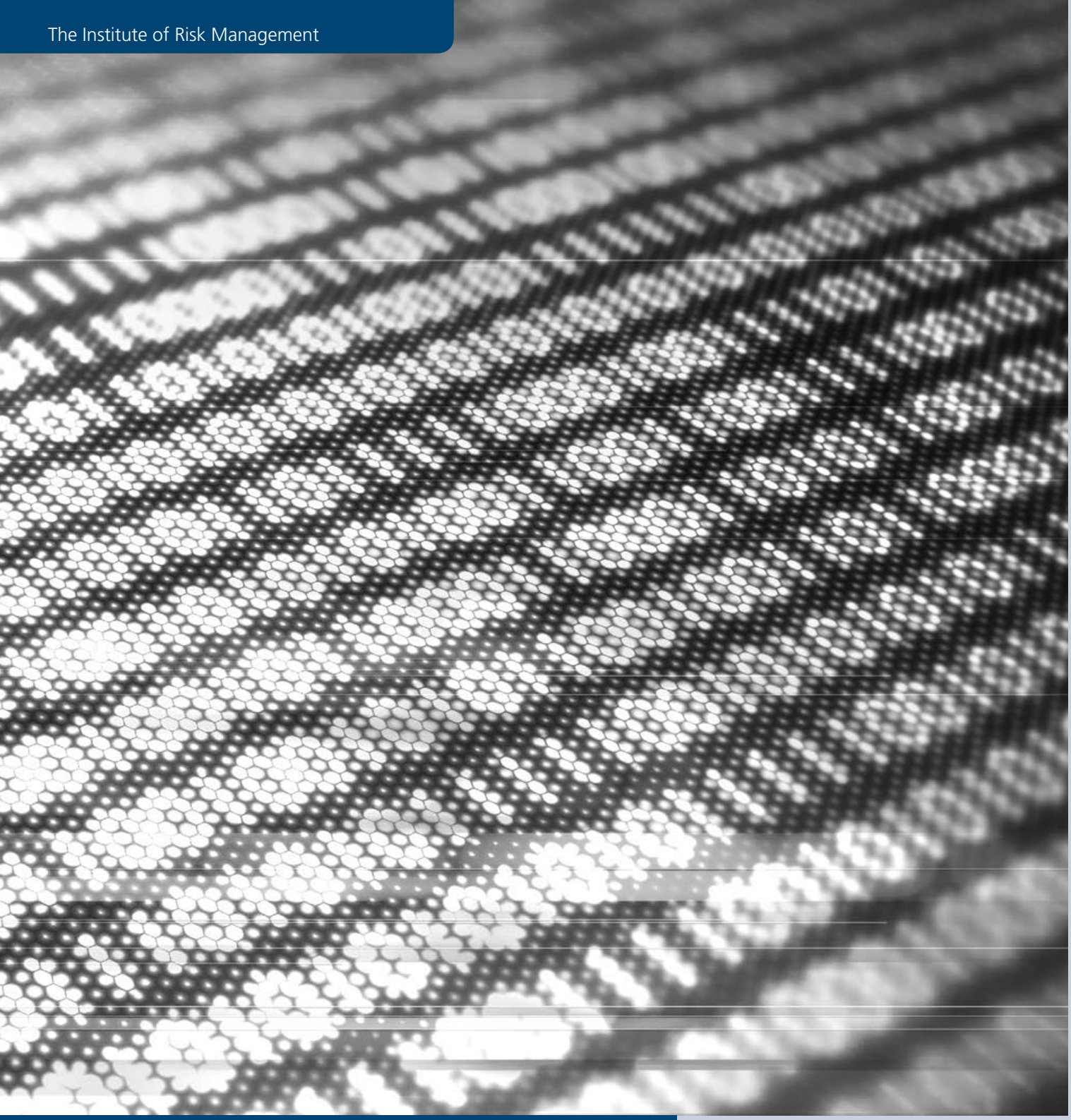
The Institute of Risk Management



Cyber Risk

Resources for Practitioners

CGI

Experience the commitment®

irm

Leading the risk profession

Our project team

IRM would like to thank the following who have contributed in various ways towards the drafting and review of this guidance. Particular thanks are due to the authors of the individual chapters whose names, where possible, are shown at the start of each chapter:

Members of the IRM RISE Special Interest Group

Alastair Allison SIRM, Zurich Insurance Group

Angeliki Chatzilia, Crowe Horwath Global Risk Consulting

David Canham, MIRM, Aviva PLC

Matt Hillyer, CIRM, TNT UK Ltd

Dan Roberts, SIRM

Harvey Seale, CIRM, Nuffield Health

Matt Willsher, BAe Systems Applied Intelligence

Carolyn Williams MIRM, Institute of Risk Management

Also with thanks to:

GCHQ

Wendy Holt, CGI

Paul Hopkins, CGI

Tim Stapleton, Zurich North America

CPNI

Roger Garrini, Selex ES

Andy Coombs, HMRC

Jennifer Wood, HMRC

Julian Phillips, JP Risk

Dorothy Maseke, UAP Kenya

Jeff Miller, Zurich Insurance Group

Chapter 10: Social media – managing risks and seizing opportunities

Angeliki Chatzilia

Introduction

"The message is the medium".

Using those words, Arthur McLuhan expressed in 1964 the idea that people tend to focus on the obvious. What McLuhan meant is that, by this focus, people largely miss the structural changes in our affairs that are introduced subtly, or over long periods of time. Whenever we create a new innovation – be it an invention or a new idea – many of its properties are fairly obvious to us. We generally know what it will nominally do, or at least what it is intended to do, and what it might replace. We often know what its advantages and disadvantages might be. But it is also often the case that, after a long period of time and experience with the new innovation, we look backward and realize that there were some effects of which we were entirely unaware at the outset[1].

What happens then when the medium is social? What are the anticipated effects it has on its users? And how does it turn into a Cyber Threat that can harm your organisation? This chapter is targeted at presenting the cyber risks and opportunities associated with the use of social media in organisations as well as the strategy and tactics that stem from best practice regarding their management.

A ubiquitous phenomenon of unprecedented impact

Two thirds of world leaders are engaged in diplomatic relations on Twitter. In 2012, the **Fortune Global 100 Companies were mentioned more than 10 million times online in one month, with most user chatter happening on Twitter.** 87 per cent of those companies are using at least one of the major social platforms to communicate with stakeholders online. As of January 2013, Facebook has more than 1.15 billion active users[2].

Although these figures demonstrate the impact and the extent of the use of social media nowadays, the vast change that they have brought to our personal, social, political and business lives has become obvious to every individual who lives in modern society.

The power of social media is such that it can be used to instigate and co-ordinate political revolutions and bring down Governments. It is not too difficult to understand what damage it could do to businesses. By shifting the power from the organisation to the individual, their use has shaped a new set of rules to the market arena arguably shaping the entire global social construct. Social and economic actors, from large multinational organisations to power exercising individuals and senior management, coexist and are part of an interactive ecosystem consisting, inter alia, of social media users and their output. Effective control over typical media channels has undergone a paradigm shift away from organisations to the ordinary person.

> The power of social media is such that it can be used to instigate and co-ordinate political revolutions and bring down Governments.

The aforementioned characteristics render social media both a valuable tool and a catastrophic threat to the ones that are affected by their use in various different ways.

On one hand, social media is considered increasingly a vehicle for organisations to interact with internal and external stakeholders: organisations are using social media tools and 'big data' platforms to build brands and communities which can engage customers in regular feedback dialogues; HR managers look for job candidates on LinkedIn and XING; R&D teams publish their development guides on corporate Wikis; and technical support personnel use instant messengers to discuss in real time critical issues with the product.

On the other hand, the extensive use of social media renders organisations subject to numerous risks that can cause serious damage to them if not managed properly. The fact that in the UK more than 51 per cent of organisations do not address social media risk as part of their risk assessment process, with 45 percent indicating that they have no plans to do so in the coming year's audit plan, reveals the perfunctory management that those risks receive. Additionally, of those that do address social media risk, 84 per cent rated their organisation's social media risk-assessment capability as "not effective" or just "moderately effective."

Due to the aforementioned reasons, social media has to be taken seriously into account by senior management, audit committees and boards of directors. These actors must ensure that they not only identify the risks and opportunities that social media engenders but also have the right risk management mechanisms in place in order to manage them as effectively as possible.

Finally, this chapter does not seek to provide an unequivocal definition or a list of what social media is and includes. As a rapidly evolving reality and uncharted territory, rather than a static list of platforms, social media is not a term that could (or should) be strictly defined. However, in the context of this chapter, social media can be seen as the means of technology-supported and internet-based interactions through which users can create, share and/or exchange information and ideas for numerous and diverse purposes, such as entertainment, business, communication, recovery after disasters and education.

More than 50 percent of social media users post personal information that exposes them at the risk of being attacked or harmed, or, in other words, at the risk of Social Engineering Attacks.

Risks

Several different types of categorisation have been proposed to classify the risks associated with the use of social media in the organisational context. However, the selection of one of them does not affect the identification of risks. According to the following classification, some events and conditions interact with each other and generate causal relationships. Therefore, a risk may be triggered by more than one event and thus pertain to more than one categories.

Social media risks are associated with the people involved in the organisation as well as with the information and the technology the organisation utilises so as to perform its operations and meet its objectives. In line with this, social media risks can be classified under the three following categories:

1. Risks that are associated with people;
2. Risks that are associated with technology; and
3. Risks that are associated with information

1. Risks associated with people

- ***Social Engineering Attacks:*** A study by Consumer Reports revealed that more than 50 per cent of social media users post personal information that exposes them at the risk of being attacked or harmed, or, in other words, at the risk of Social Engineering Attacks[3]. These attacks occur when posted information, which can be confidential, sensitive or useful in other ways, is used by a third party who subsequently uses it for malicious purposes. The information can refer either to the individual or to the organisation the individual works for and the attacker can exploit it in various ways. For example, such an attack might be used to gain access to an organisation's assets by coercing an employee or consumer to provide user IDs and passwords or by coercing the individual to execute a virus or Trojan.

- ***Account/identity hi-jacking and weak authentication:*** It is common practice for organisations to use challenge questions in order to validate the identity of people who are using the corporate or personal social media pages or other corporate IT systems. However, many times the answers to these questions can be found on the individual's own social media page or profile. Indeed, a Microsoft-Carnegie Mellon study reveals that 28 per cent of the people who are known and trusted by the study's participants could guess the correct answers to the participants' challenge questions. However, even

people not trusted by the participants had a 17 per cent chance of guessing the correct answer to a secret question after accessing their social media profile[4]. As it becomes evident, the fairly basic methods and simple password controls that social networking sites use in order to verify a users' identity render quite easy the creation of a 'fake' organisational account; or give the ability to an individual to pretend to be another individual; or to take control of an organisation's page in social media. This tactic is commonly known as account or identity hi-jacking and its consequences can be severe for the subject of the hi-jacking.

Last February, Burger King faced a relevant social media problem. The company's Twitter account had been hacked — its name had been changed to McDonalds and its background replaced with an image of Fish McBites. In the hour it took for officials to regain control, hackers proceeded to send 53 tweets to the burger chain's more than 80,000 followers, ranging from the mildly funny ("if I catch you at a Wendy's, we're fightin!") to the patently offensive ("We caught one of our employees in the bathroom doing this...," with an image of a drug user shooting up)[5].

- ***Oversharing and Exposure of Unprofessional Employee Behaviour:*** One of the most revealing examples of this risk is the case of Domino's Pizza. The company had a shocking experience in April 2009, when two employees posted on YouTube a video that showed them contaminating sandwiches and pizza with body fluid. The video was spread through YouTube and other social media all over the Internet, bringing very quickly the company in front of a significant public relations problem. As Domino's spokesman Tim McIntyre noted, "Even people who've been with us as loyal customers for 10, 15, 20 years are second-guessing their relationship with Domino's, and that's not fair."[6]

Apart from that example, oversharing of corporate information by employees can also happen unwittingly. It is true that a large number of social media users post information about their work. A recent study of Twitter users found that 62 per cent of them tweet about their work, with more than one in 10 doing it daily[7]. Additional leakages can come from contractors, vendors, partners, and affiliates. As it will be explained further below, such behaviours can expose the organisation to data breaches and loss of confidential information, the implications of which that can be staggering for the organisation.

- Candidate screening: social media sites are increasingly used by employers in order to check candidates' profiles for additional information. Nevertheless, by checking these sites the employer may end up yielding information that, although being publicly available, the candidate has not volunteered to share with the company. As a result, there is a possibility that the disclosure of a candidate's race, religion, gender, age or sexual orientation can wrongly exclude him or her from getting hired at a position they are absolutely qualified to cover in all respects.

  From a different perspective, there is also the risk that the information provided online do not reflect the actual qualifications that the candidate has obtained. Inflated qualifications or a doctored photograph could lead employers to make incorrect assumptions and recruit the wrong people.
- ***Decisions on Dismissals:*** The few cases of dismissals that have occurred in the UK due to inappropriate use of social media by employees indicate that whether a dismissal is considered fair or unfair at a legal level depends mostly on the context within and the conditions under which it occurs. Recent Acas (Advisory, Conciliation and Arbitration Service) guidance indicates that social media misconduct should be dealt with in the same way as "normal" misconduct[8]. Clearly, then, a determining factor is the employer's implementation of a social media policy and how the employee's behaviour fares against this. Hence, as with all dismissal decisions, any that involve information from social media sites should be reviewed carefully by the HR and legal departments of the company. In particular, companies need to consider both their HR policies and their social media policies in light of the possibility that any dismissal or workplace dispute may become public very fast. In the absence of clear and well-articulated social media policies, the company would face the risk of facing legal consequences, payment of fines or public discontent.

  There are several stories that prove how employee dismissals can go dramatically awry in the era of social media. For example, Applebee's waitress Chelsea Welch was fired for posting a photo on Reddit that showed a customer receipt inscribed with an anti-tipping message from a pastor: "I give God 10%. Why do you get 18?" Between the original Reddit post, Welch's subsequent article for the Guardian and a flurry of on- and offline coverage, Applebee's found itself at the centre of a firestorm that gave everyone, from labour organisers to social media evangelists something to agitate for and feel annoyed with[9].

There are several stories that prove how employee dismissals can go dramatically awry in the era of social media.

- ***Productivity and Professional Standards:*** According to a study conducted by uSamp in March 2011, social media is listed as one of the causes for approximately 60 per cent of work interruptions[10]. Such statistics increase even more organisations' concerns regarding the impact of social media on their employees' productivity and nurture the impression that social media captures their attention and leads to the waste of valuable time. Undoubtedly, loss of productivity will occur if social media is mismanaged by the organisation and its people.

  Also, inadequate use can undermine professional standards, because social networking at work can blur the lines between personal and professional life. Finally, there is also the possibility that as employees connect with one another on social media hostile work relationships may be created. This can happen if some employees get offended by information they find on their colleagues' profiles.

  In order to deal with those issues, some organisations decide to establish policies that prohibit employees from using social networking sites and block their access to them from corporate devices. However, the effectiveness of such measures is questionable at best. First of all, it is probable that employees will still be accessing social media sites from their own devices. Most importantly though, such measures can harm the company, because employees will not be able to utilise social media to reach customers and seize a wide range of other opportunities.

- Physical Safety: Online activity can lead to actual physical attacks if users of social media reveal personal details such as their address, family details or location (either directly or indirectly). The likelihood of this risk materialising increases when it comes to people that have significant roles or key positions in society, politics and the business world.
- Governance: The option of personal and direct internal communication that social media provides to the employees of a company can undermine the norms and lines of authority that exist among different levels of the hierarchy and, thus, affect negatively the effectiveness of the organisational structure and the quality of administration. Of course, such a risk is more likely to occur when social media is used by a critical mass of employees that communicate through it with each other.

One of the major risks that organisations face as pertains to social media is the fact that they cannot control what is posted about them online.

2. Risks associated with Technology

- ***Malware and viruses, flash vulnerabilities, and XML injections:*** One of the most common ways in which hackers gain access to passwords and sensitive data, as described above, is through malicious links posted on social media sites. Therefore, uncontrolled browsing and access to social media web sites and applications provide the opportunity to would-be attackers to direct malicious content to an individual user or lead him to downloading malicious content from a compromised or malicious website. After all, according to a survey performed by the Ponemon Institute, computers that are used to access social media websites face a greater risk of being hit by a virus or other malware[11].
- ***Audit control:*** The content of the data transfers that are made through social media cannot be easily audited. Moreover, organisations ignore the motives and intentions of social media users who store information that refers to their brands. This inability to monitor or record communications can also disable organisations to enforce copyright controls if they need to.
- ***Content Control:*** One of the major risks that organisations face as pertains to social media is the fact that they cannot control what is posted about them online. Indeed, social media outlets typically involve frequent and far-reaching exchanges with consumers and customers. Hence, a simple message or consumer complaint handled poorly will be seen by many people. Failing to control the accuracy and integrity of such exchanges or even limiting the interaction by taking a post offline, could quickly damage an institution's reputation and brand.

  In addition, unfavourable changes to products and services may also return to haunt institutions through social media. For instance, a prominent bank that announced plans to charge new fees for using debit cards was forced to withdraw those plans in the midst of a flurry of consumer criticism, much of which was escalated through social media.
- ***Continuity:*** As social media is used more and more by suppliers and vendors to collaborate and coordinate with each other as well as by companies to reach their customers, the consequences of an attack against the social networking sites that an organisation utilises to perform its operations become discernible. More specifically, the continuity of the organisation will be radically affected if these sites are rendered unavailable and, thus, service will be lost.

- ***Technical fault:*** The vulnerability of some social media sites to technical faults can result in a failure to implement the user's privacy settings. In this case, information that is confidential, personal or sensitive in other ways may be released.
- ***Bandwidth:*** Ponemon Institute recently surveyed over 4,000 IT security leaders in 12 countries and, according to their answers, one of the top two negative consequences of widespread social media use is reduced IT bandwidth (77 percent) – a fact which increases costs. In the context of an organisation, if there is lack of proactive management and adequate planning, insufficient bandwidth will cause problems to all the services that rely on the bandwidth[12].

3. Risks associated with information

- ***Reputation:*** Perhaps the most damaging potential impact of social media is the one it can have on the reputation of an organisation or an individual. Employees, customers, suppliers and vendors not only can be an organisation's greatest ambassadors, but also can undermine its brand and public image. At the same time, social media users can post defamatory comments about a business and its products – or services – and then share it with each other. After all, no one can control or change what is posted online.
- ***Legal and regulatory risks:*** The fact that content is posted, accessed or distributed by users or employees through the organisation's social media pages renders the organisation subject to certain obligations regarding compliance with regulation and certain legal frameworks. Failure to comply with such schemes can create financial and legal liabilities to the organisation. Exposures to legal liability can derive from, inter alia: slanderous, libellous, or defamatory comments; leakage of sensitive information; online bullying; and breach of intellectual property rights.

- ***Crisis Management:*** Cases such as that of the Arab Spring have demonstrated how extremely powerful social media can be in serving as a vehicle through which pressure groups form and gain voice. In a crisis situation, virtual pressure groups can be created so fast that the organisation will be unable to respond promptly, whereas an inappropriate management can aggravate both the crisis and its consequences.
- ***Data Leakage:*** In the era of big data, organisations receive, produce, edit, share and store a massive amount of information on a daily basis. According to the 2013 Information Security Breaches Survey in the UK, 14% of large organisations had a security or data breach in the last year relating to social networking sites[13]. From confidential documents and internal communication to trade secrets and intellectual property, data can be leaked and even become publicly available via social media websites. Once this happens, it will not be possible to fix the damage by completely deleting what has already been posted online. Data breaches take place when employees accidentally or deliberately send valuable corporate data to destinations outside of the organisation's network borders.

From many perspectives, the consequences for the organisation can be disastrous. If the company's competitive advantage is based on the information leaked, a data breach could damage irreversibly the company's strategy and, as a consequence, its financial performance. Moreover, a disclosure of client information can lead to loss of trust and confidence towards the organisation from the clients' side or cancellation of cooperation between the two parties. Finally, other potential implications of inadvertent information leakage are the detriment of its reputation or the failure of the organisation to comply with information security laws and regulations.

HMV, the international media retailer, has experienced a relevant traumatic data breach incident in the past. In January 2013, a disgruntled social media manager hijacked one of the company's social media accounts and made available to the public details about recent layoffs and mismanagement[14].

> Companies need to have policies that set guidelines regarding what acceptable use of social media means to them and their employees.

Responses to Risks

None of the myriad risks associated with social media use can be eliminated completely. However, taking a thoughtful approach and structured approach to understanding and assessing the risks and then developing and implementing a comprehensive plan will reduce significantly an organisation's susceptibility.

1. ***Development of a social media policy:*** Companies need to have policies that set guidelines regarding what acceptable use of social media means to them and their employees. These policies should address areas such as employee use of social media at work, social media use during employee hiring or termination, and vendor management policies. In addition, policies must include all the types of sites and channels that the term 'social media' refers to, such as YouTube, Pinterest, Google+ and micro-blogging sites, instead of focusing only on the most obvious media, such as Facebook and Twitter.
2. ***Engage a multidisciplinary team:*** Many organisations mistakenly think of social media as an IT or marketing problem. Because social media activity can affect a wide range of departments and functions, representatives from all the affected groups must participate in order to address the issues related to social media. An effective strategy brings together senior members of human resources, legal, IT, marketing, risk management, public relations, compliance, audit, and any other affected function. The team should be formally chartered so that each person understands his or her role and responsibilities. A project or programme manager should help the team track and maintain progress.
3. ***Training:*** All levels of hierarchy must receive proper and regular training on how to implement, monitor and enforce the guidelines that the policy has set out. However, top management, brand managers and social media page administrators have to receive tailored training, as they have key roles as ambassadors of the organisations at an external level and as leaders that define the tone-from-the-top at an internal level. The content of the training sessions must include security and compliance issues, as well as more advanced themes, such as using social media for sales and improvement of internal workflows. In addition to this training, companies can also take advantage of the online courses and webinars for users that some of the best social media tools now come equipped with.

4. ***Careful handling of customer complaints:*** social media pages nowadays have in many cases replaced the conventional customer service helplines. At the same time, the amount of feedback, reviews and complaints that companies' see posted about their brands and products on social media is massive and happens on a daily basis. Because of the fact that both this information and the companies' responses take place in front of the "eyes" of other social media users, careful handling is more than necessary. Some companies have made situations worse by simply deleting negative posts or tweets. Others have engaged in online arguments with users on social networks, unwittingly creating bad publicity. The better strategy though is to have a measured response, informing the user about what is being done to address his or her concerns. If the issue is particularly complicated, the dialogue must continue to a one-to-one basis, either on the phone or via email/message.
5. ***Review the terms of use of social media sites:*** Another important factor that has to be taken into account is whether the organisation understands and follows the terms and conditions of the social media it uses. This is particularly important when running promotions and competitions, as in some of these sites, not complying with their rules can mean that your page risks being removed.
6. ***Monitoring of the company's own pages:*** A company's social media mitigation strategy would be incomplete without the company actively monitoring potential social media activities that may expose it to risks. More specifically, attention must be paid both to the content generated by followers and friends of the company's social media accounts and to that posted by employees. In these terms, the company's policy must be clear about who is allowed to publish messages on behalf of the company. The organisation can also keep track of social media issues related to it by using social customer relationship management (CRM) tools.
7. ***Keep access as low as possible:*** Ensure you are using a positive information security model logically and administer privileges with a 'least-access-necessary' mindset. Less people with access to sensitive data both from a network perspective and a logical access perspective significantly reduces your risk in losing data through a social engineering attack.
8. ***Avoid the use of simple passwords:*** The most common password in 2012 was still "password"[15]. Sometimes, an effective password is the only barrier standing between an individual or organisation and a cyber-attack. Therefore, it is important that both the corporate and the personal accounts of an organisation and its employees are safeguarded through strong passwords. In addition, as highlighted above, it is essential that the people who know the company's passwords are limited to a necessary number and known by the company.

The most common password in 2012 was still "password".

Opportunities

The advantages of social media when used in the right way are multiple:

- ***Communication with a massive audience and a global market:*** According to a recent study by Burson – Marsteller, 80 per cent of social media users prefer to connect with brands through Facebook[16]. This fact gives an idea of the potential that businesses can unlock if they utilise social media effectively in order to advertise and promote their brands. More specifically, social media can serve as a vehicle for them to reach a massive global audience in a direct, interactive and – usually – free way.
- ***Continuous improvement and Innovation:*** The feedback and criticism that a business receives through these channels nurtures and orientates efforts towards progress and continuous improvement. In this way, the business understands its customers' needs, attitudes and experiences and provides new or improved products and services accordingly.

  When Gap used Facebook to announce their plans for a new logo a few years ago, it was hit with a massive amount of negative comments. However, Gap managed to turn the situation around and make the most out of it. More specifically, not only did the company listen to the negative comments regarding their new logo, but it also did something essential about it. After trying to alleviate the situation by giving fans the opportunity to submit their ideas for a better logo, Gap decided to revert back to the logo they had had for more than forty years. In this way, Gap established a new sense of trust with their community, which feels as though it is now part of the logo and the brand. In addition, by introducing the new logo online before it went out, Gap saved the high expenses associated with rebranding their stores and advertising.
- ***Digital Word-of-Mouth:*** When existing customers share positive comments or experiences regarding products or services, they can inspire the confidence of new customers and be an important deciding factor for choosing a company over its competitors.
- ***Enhanced relationship with clients and consumers:*** The information gathered through social media enhances businesses' market intelligence and enables them to understand profoundly their relationship with consumers, while the digital intelligence acquired informs the marketing, sales and media relations activities. Retailers, for instance, are collecting data from multiple social media sources in an effort to offer their consumers products that meet more closely their personal goals, such as a healthier lifestyle. Furthermore, insurance companies are combining customer information gathered through social media with real driving data collected from car censors so as to tailor their policies and premiums in ways that reflect real risk and are not based only on the criteria of age, gender and geography.

- ***Talent:*** Acceptance of social media in the workplace could serve as a criterion for talented candidates to pick a specific organisation for employment instead of other employers who are not embracing this access. At the same time, human resources departments take advantage of social media as a tool for recruiting new talent.
- ***Crisis management:*** social media can be used by governments, organisations, mainstream media, and the public to make the flow of information instant (and instantly helpful) when help is needed most. For example, one Facebook user created a Hurricane Sandy news page that received 191,000 likes and that dispensed loads of information critical for those wanting to know which areas were safe, to identify the where their friends and family are, and to stay aware of the progress of relief efforts.

  In the case of organisations, social media can help them prevent a flow of false, misleading or negative information by replying timely and effectively to certain events and crises. "If someone searches your brand, you want them to see the following results page: your paid ad, your corporate website, your blog, Facebook page, YouTube channel, LinkedIn, your tweets and Twitter account, says Lindsay Durfee of PR/PR. "Because now you have taken up almost all 10 spots on the search results pages of Google, Yahoo! and Bing. Customers searching for you will see everything you have to offer instead of websites trashing your organisation."

  Besides, the more active a company is in social media, the more "friends" and "fans" it will have. As Erik Deckers, author of the books Branding Yourself and No Bullshit Social Media, notes, "these people may be able to help a company through a crisis. Instead of relying only on internal staff to help mitigate the damage, the company will have a group of consumers that may do some work for them."
- ***Coordination in the context of the extended enterprise:*** Initiators and intrapreneurs are not just using social media to make their efforts more transparent and accessible; they are using these platforms to improvise and organise new ways to get the job done. They are using these tools and technologies to add value to existing processes or to create new "just-in-time" processes (and programmes) that the C-suite and other senior managers had never envisioned. Social Media inside and out of the enterprise lowers the costs and increases the power of individuals to productively coalesce and coordinate on their own initiative.

  For example, implementing a multi-media proposal developed by MIT students, a company's supply chain and procurement teams utilized LinkedIn, private Tweets and cut-and-paste Sharepoints to quickly coordinate go-to-market product changes with key vendors. By overcoming diverse issues, such as incompatibility among communications networks and the lack of a proactive IT department, the ad hoc network enabled suppliers to transparently coordinate and collaborate with each other as well as respond to their customers' requests.

> Before, while and after an organisation builds its social media strategy, it is essential that it listens to what is being said on social media.

How to seize opportunities

As every industry, brand and organisation is characterised by specific needs and attributes, best practices regarding social media cannot be generalised. Rather than being a panacea to heal the gaps and possible mistakes that companies' conduct in the context of their marketing and corporate strategy, social media should be seen as a tool that facilitates the communication of an organisation with its stakeholders and empowers it to seize the wide range of opportunities that the digital era has to offer. In order to achieve that though, there are several parameters that organisations should have in mind. These are the following ones:

1. ***Listening is essential:*** Before, while and after an organisation builds its social media strategy, it is essential that it listens to what is being said on social media. Listening must not be limited to the competitors and the target audience of an organisation, but it should rather include all the wider conversations that take place on social platforms.
2. ***Analyse what you "hear":*** By listening to its current or potential audience, the organisation collects for free data that can be distributed to utilised by its various divisions: from sales and marketing to production and finance. In addition, it enhances its database in a way that renders much easier the conduction of benchmarking analysis as well as the comprehension of what the current trends and the main influencers are.
3. ***Build the right strategy for your organisation:*** As Kelda Wallis of Tempero Social Media Management highlights, "the key in determining your social media strategy is to understand your social purpose. In other words, find what you can give to your audience and how you want to connect with it". In doing so, the organisation has to create strategy that is based on the value it can deliver to its customers and fully considers the appropriate use of social media channels in order to match its unique attributes. Finally, the social media strategy must not be isolated from the corporate one. On the contrary, is should embrace and support all the components and functions of the organisations in the best possible way.
4. ***Communicate your social media strategy adequately:*** All levels and employees of the organisation must be aware of how social media are utilised by the organisation. However, it is equally important that they are communicated what they are allowed and not allowed to post about the brand, the works place or their colleagues online. Also, it is essential that top management gives the right tone-from-the-top by embracing the social media strategy and policy and by being the ambassadors of the brand on the different platforms.

Content posted and the manner in which the organisation uses social media must be monitored systematically in order to assure that they are aligned with the corporate strategy and objectives.

5. ***Governance:*** Each division must know how it can utilise social media in order to take full advantage of it, but it must also understand that only the social media team gives permission for content to be uploaded online and to coordinate social media-related actions.
6. ***Monitoring:*** Both the content posted and the manner in which the organisation uses social media must be monitored systematically in order to assure that they are aligned with the corporate strategy and objectives. In this way, if any deviations are observed or an unexpected event takes place, the organisation will be in a position to take action timely and effectively.

Conclusions

To sum up, social media can be a double-edged sword for organisations. On one hand, social media can be a very a valuable business weapon, as it allows the organisation to communicate in a personal, direct and costless way with its stakeholders as well as to utilize a wide variety of multimedia to reach its audience. In the virtual world that social media delineate, space is not a limit either. A brand can become present in markets it had never imagined of, whereas data can be analysed so as to meet the needs and characteristics of new clients. Finally, the, company can deploy social networks to administrate and organise itself in a more cohesive and direct manner and hence perform its operations in a timely and efficient manner.

On the other hand, social media is still an unchartered and constantly evolving environment that can sometimes be difficult to use safely and productively. Risk managers and senior management have to ensure that the proper measures are in place to guard corporate data, secure connections and protect against increasingly common malicious attacks that take place via social media.

According to the analysis realised in this paper, the answer to the cyber threats the organisations are exposed to due to the use of social media is not to ignore social platforms or ban their use within the organisational premises. Organisations must rather realise the uniqueness of the advantages that this tool can offer them and make sure that they allocate the right resources through an adequate strategy so as to turn social media into a vehicle through which they deliver value to their audience.

Questions for Executives

Are you using social media in your organisation (Facebook, Twitter, LinkedIn, etc…)?

If the answer is no, think about it again before you reply and reflect on the next question.

How do you track what your employees, your customers and the public say about your organisation on social media?

How do the various departments/divisions in your organisation use social media in the context of increasing sales, supporting operations and internal communication?

Have you developed a social media strategy? If yes, how do you verify your employees understanding of it?

Have you trained your employees so as to increase their awareness of risks and opportunities associated with social media use?

What is the structure of roles and responsibilities regarding social media in the context of your organisation?

How has your organisation made sure that it is able to manage a crisis related to a social media incident (e.g. an employee dismissal gone public via Twitter)?

Bibliography

1 McLuhan, Marshall. Understanding Media: The Extensions of Man. New York: McGraw Hill, 1964.Federman, M. (2004, July 23). What is the Meaning of the Medium is the Message? Retrieved 09-08-2013 from **http://individual.utoronto.ca/markfederman/article_mediumisthemessage.htm**

2 Burson – Marsteller Twiplomacy Study 2013: **http://twiplomacy.com/twiplomacy-study-2013/**

3 **http://www.consumerreports.org/cro/news/2010/05/consumer-reports-survey-social-network-users-post-risky-information/index.htm**

4 Robert Lemos, "Are Your 'Secret Questions' Too Easily Answered?," Technology Review, May 18, 2009, **http://www.technologyreview.com/web/22662/?a=f**

5 **http://www.bbc.co.uk/news/world-us-canada-21500175**

6 **http://www.nytimes.com/2009/04/16/business/media/16dominos.html?_r=0**

7 Chloe Albanesius, "8 Percent of American Web Users on Twitter, Pew Says," PCMag.com, Dec. 9, 2010, **http://www.pcmag.com/article2/0,2817,2374100,00.asp#**

8 **http://www.acas.org.uk/media/pdf/f/q/1111_Workplaces_and_Social_Networking-accessible-version-Apr-2012.pdf**

9 **http://www.huffingtonpost.com/alexandra-samuel/when-hr-decisions-become-_b_2664001.html**

10 **http://harmon.ie/Company/PressReleases/press-release-may-18-2011**

11 **http://www.websense.com/content/ponemon-institute-research-report-2011.aspx?cmpid=prnr11.10.06**

12 **http://www.websense.com/content/ponemon-institute-research-report-2011.aspx?cmpid=prnr11.10.06**

13 **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf**

14 **http://www.huffingtonpost.com/alexandra-samuel/when-hr-decisions-become-_b_2664001.html**

15 **http://gizmodo.com/5954372/the-25-most-popular-passwords-of-2012**

16 Burson-Marsteller Global Social Media Check Up 2012: **http://burson-marsteller.eu/innovation-insights/global-social-media-studies/**