Social Media Security Culture

The Human Dimension in Social Media Management

Caroline Oehri, Stephanie Teufel
University of Fribourg
international institute of management in technology (iimt)
Boulevard de Pérolles 90
1700 Fribourg, Switzerland
caroline.oehri@unifr.ch, stephanie.teufel@unifr.ch

***Abstract*— Social media provides both opportunities and risks for any organization. Secure integration of social media platforms in organizational ICT infrastructures tends to be focused mainly on technical aspects. Social media security management usually ignores the human dimension, but protection can only be achieved through a holistic approach. Social media security culture must be part of the overall organizational culture. From a survey conducted to determine social media guidelines, a management model was developed for creating, monitoring and controlling social media security culture. The management model will be mapped to an assessment and reporting tool.**

Keywords - social media security, social media culture, security awareness, social media and security management

I. Motivation

Social media provides opportunities and risks for both industry and government. Employees' behaviour on social media platforms can have either positive or negative effects for a company or an administration. Secure integration of social media platforms in organizational ICT infrastructures is mainly focused on technical aspects. Social media security management usually ignores the human dimension, but protection is only possible through a holistic approach. Rules of conduct appear to be essential.

Rules of conduct appear to be essential as this will form the basis to establish a specific culture in line with the organization. Appropriate social media guidelines are obviously required, although studies have shown that only rudimentary guidelines have been established so far. The social and cultural aspect of existing technical and organizational procedures can be improved in order to increase security awareness (cf. [1] and [2]). This is especially the case regarding the use of social media tools. Socio-cultural measures will increase the responsibility and security awareness of social media users within an organization, thereby improving its level of security.

In this paper the human aspect of the social media security management process will be discussed. Firstly a short introduction on opportunities and risks is given to outline the motives. This is followed by a description of a social media survey, from which the social media guidelines are derived. These guidelines then form the basis of a management model for creating, monitoring and controlling a social media security culture.

II. Social Media – Opportunities and Risks

The intrinsic capacity of social media tools to spread news "virally" and globally can be used positively, but can also lead to serious reputation damage, loss of confidence and leakage of confidential material. They present both opportunities and risks at the same time [3]. Employees can cause considerable harm to themselves and their business organizations through social media activity without due reflection. It is important to note that the boundaries between private and business activities are becoming blurred.

In 2011, an online survey conducted by McKinsey received responses from 4,261 executives on the opportunities provided by social media. Their responses indicated exceptional advantages in terms of cutting communication costs, fast and effective access to internal and external experts and increased marketing effectiveness [4].

Social media requires clear procedures for use in order to benefit from its advantages and avoid the disadvantages. Interactive and direct social media communication with customers, colleagues and business partners can provide an important impetus for business processes. At the same time, customer retention and loyalty can also be increased and strengthened. It encourages open dialogue among employees outside of hierarchical structures. Social media profiles are helping to make contacts with partners and colleagues more personal and intimate. This creates a collective consciousness among employees and a strengthening of business relations, thereby improving the working environment and increasing motivation. Public criticism of companies can be minimized through open, simple, flexible and interactive communication, which encourages customers to approach the company directly rather than criticize it publicly.

The benefits gained from these opportunities depend on the behaviour of individuals on online platforms and the information that is shared or spread publicly via such platforms. A high level of security awareness is needed to prevent potential hazards, such as damage to reputation through unprofessional conduct, loss of control, cyber mobbing, social engineering and malware attacks. Different studies pointed out that many organizations already have become a victim of social engineering attacks, cf. [17] for example.

A survey by the Sophos Group showed that 72% of interviewed companies believe that their employees can cause harm by inappropriate and unprofessional behaviour on social media platforms [5]. They also fear losses of productivity and of confidential data as well as malware and spam attacks through social media platforms. These safety concerns can be addressed through active security awareness. Adequate, valid and safety-conscious behaviour should be incorporated through a holistic approach. Hazards can be minimized and opportunities maximized if all employees are able to adopt an appropriate online presence and conduct through specific training and procedures. Figure 1 below shows the most commonly cited safety concerns with respect to social media that emerged from a survey by Clearswift.

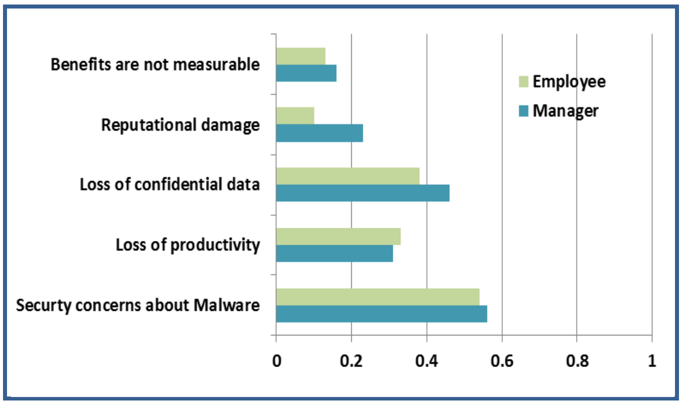

Figure 1. Security concerns of companies using social media, according to [6].

A recent survey among some of the largest Swiss companies showed that nearly two-thirds of the companies were active on social media platforms. Only 22 percent of them, however, had developed a social media strategy and only 30 percent had specific social media communication guidelines with rules for the appropriate use of and behaviour on social media platforms. At least 41% of the companies without social media guidelines were planning to introduce them [7]. Rules of conduct therefore appear to be essential.

III. Culture and the Human Dimension

When it comes to social media tools, the human factor assumes even greater importance than with standard information security. This was reconfirmed by IDC Europe in 2011: a published survey on IT Security in Germany showed that company employees are still the weakest link in the IT security chain [14] (see Figure 2).

When talking about corporate culture, this entails the employee's view of the organization. From a management theory perspective, culture can be viewed in a functional or a cognitive-interpretative way [8]. The first sees every organization as having its own culture, whereas the second views every organization as a culture. The research work introduced in this paper follows the theory of [9], which integrates both approaches. Corporate culture is therefore a dynamic collective phenomenon. It can be influenced or even designed by the management of the organization.

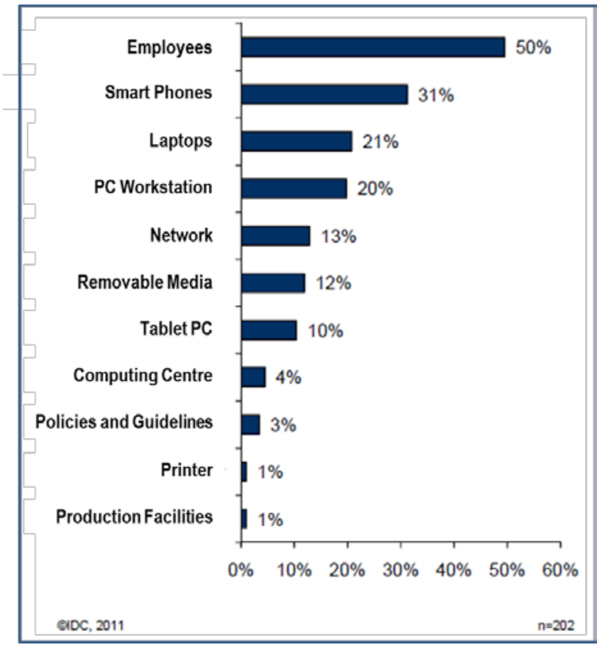

Figure 2. The weakest links in the IT security chain [14].

An important aspect of an organization's culture is the fundamental hypothesis characterizing its members, i.e. their behaviour and relationships. In terms of social media, this particularly concerns the way they act and communicate internally as well as externally.

Corporate culture is therefore expressed in collective values, rules and organizational knowledge. Such rules and values undoubtedly influence employees' habits and corporate culture certainly has a direct influence on the performance and strength of an organization. Culture is not static. It is a dynamic process which is influenced by the environment (e.g. technical developments or changing legal situation) and most of all by the members of an organization, especially its management and board of directors.

IV. Social Media Guidelines

Meaningful social media guidelines are practical rules of conduct which allow the new technologies to be used safely. They are intended to appeal to common sense and encourage safe, value-adding behaviour.

Therefore, towards the end of 2011 an investigation among Swiss organizations and companies was launched to find out how they act in the social media world. The survey has shown that 42 percent of responding companies / organizations have no guidelines of any kind for the use of social media platforms [2]. The survey included some of the best-performing Swiss companies. Both the opportunities and the threats of social media tools were highlighted and it became evident why social media guidelines represent a useful security document for any company. Some companies have already developed such guidelines, which should help their employees make sensible decisions about their "online activities", to protect themselves as well as the company.

Existing guidelines were then analyzed to discover the necessary requirements for a compendium of adequate rules. Thus a survey was conducted by directly contacting 138 of the best-performing companies to gather information on social media guidelines. Based on a return rate of nearly 37 percent, a qualitative content analysis was performed, referring to Mayring’s technique [10], which was evaluated using quantitative methods.

Existing guidelines were parsed and compared in order to obtain quantitative statements about frequencies and priorities. The norms and rules most frequently used in existing guidelines were thereby identified and various exposed security gaps were also clearly revealed. It was therefore possible to establish the relevant rules that are essential to all social media guidelines. The most cited norms are shown in Figure 3.

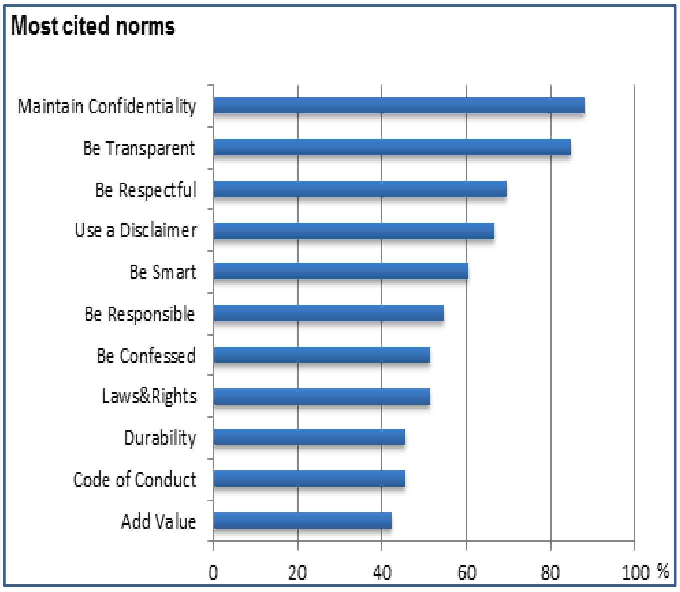

Figure 3. Most commonly cited norms [2].

The most cited norms were compared to recognized risks and threats. Existing security gaps were then highlighted to indicate the risks that still needed to be addressed. The risks and threats were selected according to a criterion of their being directly controlled and influenced by everyone. If the threats were not controllable and avoidable by all employees, a code of conduct would be pointless.

It was interesting to discover that most existing social media guidelines did not mention the high risk posed by social media in relation to malware. Warnings against social engineering, malware and spam were only given in twelve percent of the guidelines, and only six percent of them recommended prudence when accepting requests from friends and clicking on links.

Industrial espionage is facilitated by the use of social engineering and malware attacks (phishing, worms, viruses, spyware, adware and trojans) can cripple entire corporate networks and steal confidential data. Therefore, in the light of the results shown in Figure 1, it is assumed that companies view malware as the biggest social media risk, but nevertheless do not provide any measures to train their employees in preventive security awareness. Increasing security awareness should be a concern of all companies, and indications of these technical-based dangers should be included in all social media guidelines. This conclusion is supported, for example, by the results of the Sophos Security Threat Report 2012, which indicates an increased rate of malware and social engineering attacks [11].

Oehri [2] has defined a compendium of standards that will serve as a template for specific social media guidelines. The standards indicate weak points and advise against the dangers posed by social media. The guidelines are intended to provide indications and are considered a prerequisite for safety awareness and an informed use of social media.

The resulting compendium contains twelve rules for appropriate use of social media platforms, to protect individuals and companies from data loss, reputational damage and malware attacks. For example, “reputational damage” is addressed by the “maintain confidentiality” rule, meaning that employees who actively use social media should take care to protect confidential data and information (the confidentiality of sensitive data). According to [16], it should be noted that social media guidelines can only be effective if they are known and understood by all employees.

The inclusion of social media guidelines in corporate culture, to ensure digital communication security, is therefore very important. Moreover, as individual use of technology for both private and business purposes increasingly merges, such guidelines, as part of the culture, help to make the personal workplace secure. This is what Talib, Clarke and Furnell refer to as an “all-round individual security culture” [12].

V. Social Media Security Management

The defined guidelines are a prerequisite for social media security management. A socio-cultural, person-centred approach based on trust and partnership, combined with appropriate social media security technology, is needed.

We all know that 100% security is neither possible nor cost effective. In information security, the costs of countermeasures must always be compared with the benefits in terms of decreased risk. This applies both to technical countermeasures as well as human measures: thus, some residual risk has to be accepted. Social media security guidelines ought to define the extent of this residual risk [1].

Social media security culture, like any kind of culture, is dynamic. It cannot simply be created and then used indefinitely without further action or modification. Business objectives as well as business environments change over time. Thus, the culture has to be continuously maintained and allowed to evolve. This is a continuous process comparable to a cybernetic model. Firstly, the current situation, i.e. the social media security culture, has to be analyzed (*Diagnosis*). This implies a target-performance comparison resulting in changes to the culture in the event of detected problems. In the case that no complications are found, then the culture should be strengthened. Necessary tasks and actions must be determined (*Planning*) and executed (*Implementation*) for this purpose. Finally, the success of this planning and implementation process has to be assessed and documented (*Evaluation*). This cycle is shown in Figure 4.

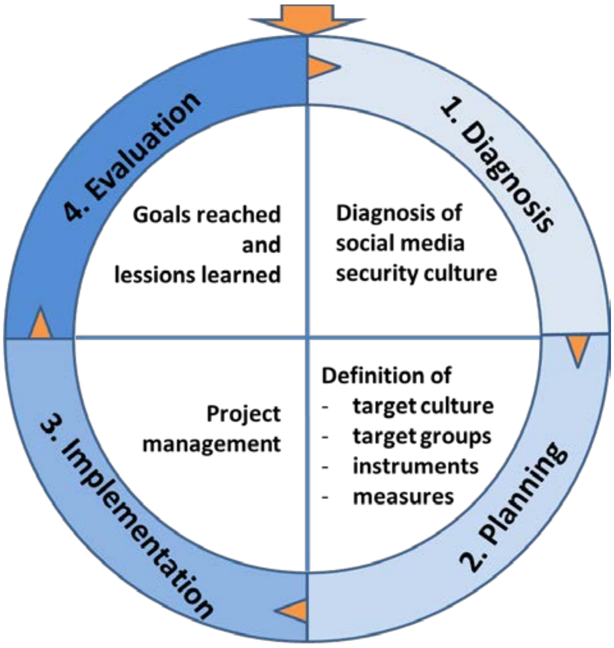

Figure 4. Social media security culture management process.

A short overview of these four management steps is provided here below.

Diagnosis As with the approach adopted for the development of information security culture [13], a set of methods is required for assessing the social media security culture in an organization.

Planning The diagnosis step examines the actual culture and its weaknesses. Depending on the particular culture, certain actions – specific to the context – must be taken to maintain or to change the culture. While an appropriate security culture can be maintained by an effective awareness programme, changing a culture involves the reengineering of all existing cultural measures.

Implementation The implementation of the planned actions is organized like any other project. It is essential to define detailed activities, responsibilities and resources, the schedule and the budget.

Evaluation Evaluation is the last step in the social media security management process. It provides valuable information about the efficiency and effectiveness of the implemented measures. It helps to improve the actions taken, to define necessary follow-ups and also to legitimate investment in social media security culture. This is especially important in relation to the following year’s budget.

VI. The Social Media Culture Assessment and Reporting Tool

In order to ensure an economical approach, training and educational measures needs to focus on areas where gaps have evolved. The four steps of the new social media security management process must be carried out with the utmost care and attention to guarantee the highest possible security level. This can be achieved by supporting the management process with an expert system.

This is where the Social Media Culture Assessment and Reporting Tool (SCART) come into play. SCART is a software system that helps to detect security gaps through qualitative evaluations using a standardized questionnaire. According to the shown social media security management process the system consists of two principal components: the Assessment-Tool and the Reporting-Tool.

Assessment-Tool The process of Diagnosis is mapped to a survey system running as a web-service. Standardized questions and answers are provided by the system. Self-evident, authorizing techniques are applied and privacy and integrity are ensured.

Reporting-Tool The process parts Planning, Implementation and Evaluation are supported by the reporting tool which is also developed as a web-service. Similar authorizing rules apply. Results of the assessment tool can be viewed and/or exported for use in other systems.

The system allows continuously verifying whether the guidelines have been adequately appropriated and applied by the staff. If security deficits are found, suitable approaches and measures need to be recommended to help build an adequate level of security awareness among employees and thereby enable companies and institutions to secure or even enhance their business process.

A standardization of these recommendations of action then can be seen as the knowledge base of an expert system based on SCART. The system architecture is described in more detail in [15].

VII. Conclusion

People are linked, form part of networks and are in constant interaction and communication with one another. Products, services and companies are discussed openly. This movement leads to an ongoing erosion of the boundaries between the private and business spheres. It has become normal to voluntarily publish likes, dislikes, opinions, photos and videos. Social media is growing in influence, but its potential and its risks are given insufficient attention. Employees can cause themselves and their businesses significant damage by thoughtless behaviour on social media platforms. Effective protection is therefore achieved only through a holistic approach combining a secure technical system with individual security awareness. Each social media user should be aware of the prevailing threats to themselves and the safety of their company. Risks and threats need to be highlighted and security protection instructions must be given.

Due to the mixed professional and private use of social media platforms, it is important to establish clear rules of conduct. Employees can work as individual corporate ambassadors and can radiate professionalism through appropriate conduct, which can impact positively on the existing corporate reputation. If employees are not educated in regard to proper social media skills, the benefits will not be gained and the disadvantages cannot be avoided. It is therefore important that users expand their background knowledge of social media in order to deal with these new media tools. The establishment of a social media security culture and the respective guidelines allow the full benefits of social media to be exploited, in both the business as well as the private sector.

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support of this work by grants from Hasler Stiftung Switzerland.

REFERENCES

[1] T. Schlienger, S. Teufel, "Information Security Culture - The Socio-Cultural Dimension in Information Security Management. Security in the information society: visions and perspectives," IFIP TC11 International Conference on Information Security, Cairo, Egypt, 2002.

[2] C. Oehri, Social Media Guidelines. Einführung von Richtlinien in die Unternehmenskultur, zur Unterstützung der Sicherheit digitaler Kommunikation. iimt University Press, Fribourg, Switzerland, 2012.

[3] P. R. Scott, J. M. Jacka, Auditing Social Media: A Governance and Risk Guide, Institute of Internal Auditors Research Foundation, John Wiley & Sons, Hoboken, USA, 2011.

[4] J. Bughin, M. Chui, A. Hung Byers, "The networked enterprise holds steady" McKinsey Quarterly, McKinsey & Company, 2011.

[5] Sophos, Security Threat Report 2011. Sophos Ltd., Boston, USA, 2011.

[6] Clearswift White Paper, Web 2.0 in the Workplace Today – Report 1, April 2010, Retrieved 26. November 2011 from http://www.clearswift.com/resources/white-paper

[7] B. Kunert, M. Berent, Social Media Studie Schweiz - Von Web 2.0 zum Online Dialog. Bernet_PR AG, Zürich, Switzerland, 2011.

[8] G. Schreyögg, Organisation - Grundlagen moderner Organisationsgestaltung, mit Fallstudien (5. Aufl.). Springer Gabler Verlag, Wiesbaden, Germany, 2008.

[9] E. Rühli, "Unternehmungskultur - Konzepte und Methoden," in: E. Rühli, A.Keller (eds.), Kulturmanagement in schweizerischen Unternehmungen. Verlag Paul Haupt, Bern, 1991.

[10] P. Mayring, Einführung in die qualitative Sozialforschung. Beltz Verlag, Weinheim, 2002.

[11] Sophos, Security Threat Report 2012. Sophos Ltd., Boston, USA, 2012.

[12] S. Talib, N. L. Clarke, S. M. Furnell, "Establishing A Personalized Information Security Culture." International Journal of Mobile Computing and Multimedia Communications (IJMCMC), Vol. 3, Iss. 1, 2011.

[13] T. Schlienger, S. Teufel, "Tool supported management of information security culture: an application to a private bank," in: R. Sasaki, E. Okamoto, H. Yo-shiura, The 20th IFIP International Information Security Conference - Security and Privacy in the Age of Ubiquitous Computing, Chiba, Japan, 2005.

[14] IDC Europe GmbH, IDC-Studie: "Abwehr neuer Angriffsszenarien, Cloud und Mobile Security sind die Top 3 Prioritäten deutscher IT Security Verantwortlicher," press release, IDC GmbH, Frankfurt, Germany, 2011.

[15] S. Teufel, B. Teufel, The Social Media Culture Assessment and Reporting Tool SCART, submitted for publication, 2012.

[16] F. Almeida, "Web 2.0 Technologies and Social Networking Security Fears in Enterprises." International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 3, No. 2, 2012.

[17] G. Sarpong: Studie: Sicherheitsrisiko Social Engineering wird unterschätzt. Netzmedien AG: http://www.it-markt.ch/News/2011/09/26/Sicherheitsrisisiko-Social-Engineering-werde-unterschaetzt.aspx