Controls Mitigating the Risk of Confidential Information Disclosure by Facebook: Essential Concern in Auditing Information Security

Ivan Ognyanov Kuyumdzhiev

Ivan Ognyanov Kuyumdzhiev,22 d-r Petar Beron st, Varna, Bulgaria

***Abstract* – Facebook allows people to easily share information about themselves which in some cases could be classified as confidential or sensitive in the organisation they're working for. In this paper we discuss the type of data stored by Facebook and the scope of the terms "confidential" and "sensitive data". The intersection of these areas shows that there is high possibility for confidential data disclosure in organisations with none or ineffective security policy. This paper proposes a strategy for managing the risks of information leakage. We define five levels of controls against posting non-public data on Facebook - security policy, applications installed on employees' workstations, specific router software or firmware, software in the cloud, Facebook itself. Advantages and disadvantages of every level are evaluated. As a result we propose developing of new control integrated in the social media.**

***Keywords* – Facebook, audit, information security, security policy.**

1. Introduction

Facebook has long been a major factor on Internet. It is used by more than 1. 15 billion users [17] for different purposes – personal (sharing images, videos, news, keeping in touch with friends or finding new ones [1] or professional (advertisements, connections with customers, recruiting job applicants [10], which makes it a place for sharing and collecting a vast amount of information.

It is common for many companies to have policies controlling employee use of computers and Internet access while at work [10]. However, many of these organizations do not properly assess the risks of using Facebook by their employees and therefore do not take adequate precautions. As a result of the lack of proper security policy, employees can intentionally or unintentionally share important information about the organization, leading to losses for the company. A common mistake is that the access to Internet is either not controlled at any level or is prohibited. These approaches may lead to:

- Lost profits - in case that the company chooses to ignore the numerous positive aspects of Facebook and block all access to the network.
- Making the company vulnerable to threats like:
  - Clickjacking [16].
  - Click fraud, Survey scams, Rogue apps [11],
  - Social engineering and botnets, External payload [12].

It is obvious that neither of these two is a solution to the problem. Countermeasures against Information leakage include use of software solutions at different level of the network – users' workstations, company router, software in the cloud.

Purpose of this article is to:

- assess the probability of leakage of company information classified as sensitive or confidential through Facebook.
- assess existing controls managing the risks of information leakage.
- propose new controls and strategy for assessing the existing control for the purpose of the audit of information security

2. What information is published and stored in Facebook

According to Facebook [13] the social network receives the following categories of information from users:

- Registration information - name, email address, birthday, gender, telephone number.
- "Information you choose to share" – status updates, uploaded photos, or comments, added friends, liked pages or websites, added a place to a story, relationship status.
- Information shared by others – photos, tags at locations, group membership.
- Other information:

□ When Facebook is used, when and which other user's timeline is visited, used keywords for searching, sentand received messages.

□ Metadata - such as the time, date, and place the user took the photo or video.

□ Data from or about the computer, mobile phone or other device used to access Facebook [9] – IP address or mobile phone number, ISP location, operating system, location, the type (including identifiers) of the device or browser and visited pages.

□ Whenever a user visits a game, application, or website that uses Facebook Platform or visits a site with a Facebook feature - URL, date and time the site is visited.

□ Data from Facebook affiliates or advertising partners concerning user’s response on ads.

A review of all the fields available for user editing though clearly shows that in the above list the following data hasn’t been mentioned anywhere that it’s actually stored with them (Facebook):

Hometown, languages spoken, a brief description (about me), friends and relatives attended events, employer, university graduates, school, religion, political beliefs, "people who inspire us", favourite music/books/movies/TV shows , preferred television, games, favourite sports, favourite teams/athletes, activities and interests, phone number – home/business/personal, address, city, neighbourhood website.

Additionally to the list can also be added and the data that is obtained through various programming (PHP, Perl, JavaScript etc.)functions - used resolution, local time, the address of the page (if any) which referred the user agent to Facebook, time spent on site, etc.

Part of this information is public. The other part (according to Facebook privacy policy) is private and its owners are able to manage who can access it. Taking into account the huge list of data stored on Facebook, it is clear that users voluntarily choose to ignore their right for privacy. An interesting fact is that the vast majority of users normally decide to share only certain piece of information, also in the most of the cases theyshare it comprehensively and accurately than partially and incorrect [1] and often reveal their true identities. Moreover they are often not concerned about the security risks [6] of this decision. These behaviours could be explained by the lack of knowledge of the possible consequences but it may have a significant impact on company in which they work if shared data is classified as sensitive.

3. Sensitive data and confidential information

Classification of information is an important part of the implementation of quality strategy for security management. Often classification of different organisations varies. According to Information Classification Policy of ISO/IEC 27001:2005 A.7.2.1 the information should be classified [14] as:

Public - Information is not confidential and can be made public without any implications for the Company.

Internal or proprietary - Information is restricted to management - approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Examples include: passwords and information on corporate security procedures, Know-how used to process client information, Standard Operating Procedures used in all parts of Company’s business, departmental memos, training materials, operating procedures, phone and email directories, marketing or promotional information etc.

Confidential or restricted – includes Client Confidential Data and Company Confidential Data. Highly sensitive or valuable information, both proprietary and personal.

Client Confidential Data - Information received from clients in any form for processing in production by Company.

Company Confidential Data - Information collected and used by Company in the conduct of its business to employ people, to log and fulfil client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. Examples include: Company business plans, Salaries and other personnel data etc.

Stanford University’s security policy defines two main types of information – non-public and public [20]. Non-public information is classified as Prohibited, Restricted and Confidential:

Prohibited Information - Information is classified as "Prohibited" if protection of the information is required by law/regulation or Stanford is required to self-report to the government and/or provide notice to the individual if information is inappropriately accessed. Examples include: Social Security Numbers, Credit Card Numbers, Financial Account Numbers etc.

Restricted Information - Information is classified as "Restricted" if it would otherwise qualify as "Prohibited" but it has been determined that prohibiting information storage on Computing Equipment would significantly reduce faculty/staff/student effectiveness. Examples include: Health Information, including Protected Health Information, passport and visa numbers, export controlled information under U.S. laws

Information is classified as "Confidential" if (1) it is not considered to be prohibited or Restricted and is not generally available to the public, or (2) it is listed as Confidential. Examples include: Student Records, Research data, Faculty/staff employment applications, personnel files, benefits information, salary, birth date, and personal contact information, Project or Task numbers etc.

Public information - All information which does not fall into one of these categories is considered to be "public".

The security policy of the [21] reveals a slightly different classification of data:

Sensitive data refers to data whose unauthorized disclosure may have serious adverse effect on the University’s reputation, resources, services, or individuals. Data protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive

Private/confidential data refers to data whose unauthorized disclosure may have moderate adverse effect on the University’s reputation, resources, services, or individuals. This is the default classification category and should be assumed when there is no information indicating that data should be classified as public or sensitive.

Public data refers to data whose disclosure to the general public poses little or no risk to the University’s reputation, resources, services, or individuals.

Analysis of the examples and definitions of sensitive, private, confidential data shows that in some cases these terms are used as synonyms. On the other hand there are obvious differences in the classification even with organisations working in the same sector. Intersections of these classifications bring us to the conclusion that sensitive, private and confidential data are defined as a key asset for the organisations and should be protected from external access, otherwise may have serious adverse effect on the organisations’ reputation, resources, services, or individuals. Many of the data recorded onFacebook could be classified as sensitive, private or confidential depending of the context. Ironically the social networks are one of the most inappropriate places for the exchange and storage of confidential information. However, their users can do it intentionally or unintentionally. Using Facebook security features, users can mark some of the shared information as “private”. This means that it should be visible only to list of friends specified by the user. This security mechanism could not be defined as reliable for two reasons:

1) Facebook Data Use Policy is a subject to frequent changes (at least 3 times for the last couple of years). There is no guarantee what decision would take a new board of directors, and thus private information today may be public information tomorrow. Furthermore experience shows that large organizations servers are target for hackers’ attacks, which sometimes prove successful.

2) Confidentiality concerns the protection of sensitive information from unauthorised disclosure. This means that if two users exchange private/confidential information onFacebook there should be a mechanism to encrypt it so it could be visible only for the two parties. There is currently no such feature which allows us to conclude that Facebook does not offer confidentiality.

To address these issues companies should define their own information classification and access permissions. Every employee must be aware of this security policy and the consequences of violating it. On the other hand violation of organizational IT security policies is a common problem in organizations [8]. Therefore The CERT Program's Common Sense Guide to Mitigating Insider Threats recommends logging, monitoring, and auditing employees' online actions [2], [3]. To meet this requirement, the organization must implement prevention, detection and corrective controls for countermeasures against information leakage.

4. Defining existing controls

An important part of any audit of information security is collecting of information about existing controls and classifying them. Limiting leaks of organizational information through Facebook can be done on 5 levels:

1) Security policy
2)Applications installed on employees’ workstations
3) Specific router software or firmware
4) Software in the cloud
5) Facebook

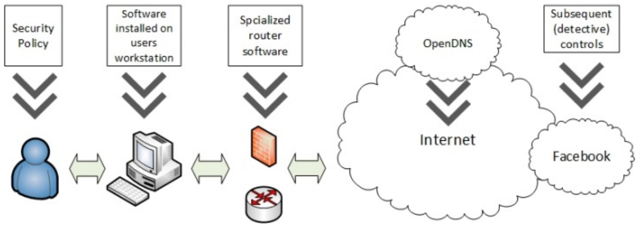
Security Policy
Software installed on users workstation
Spcialized router software
OpenDNS
Subsequent (detective) controls
Internet
Facebook

Figure 1. Controls mitigating risk of disclosure of sensitive data

1) Security policy is an essential preventive control. Every company must create clear and detailed classification of the information in use. Compliance with security policy should reduce unintentional misuse of sensitive data. Security policy defines:

- Instructions for classifying information and access rights of the employees. The policy should also define restrictions on the use of this information by people who have access to it.
- Definition of the concept of ownership of data, as well as requirements necessary to create, modify or delete information. Without these guidelines security management in large

organizations is difficult as it may be that there is no one responsible for key data.

As stated above even the most detailed and well spread policy cannot guarantee information security. But IT security training and awareness has been shown to be an important proactive action to decrease security policy violations [4],[7].

2) Applications installed on employees workstations.

This type of software can be divided into two types - plugins for browsers and parental control software.

Plugins for browsers can provide options for centralized management of filter criteria (if the plugin is developed by the company). Unfortunately, it is possible for employees to stop the plugin or use another browser, which makes this control unreliable.

There are many software solutions for parental control. Some of the best [18] paid applications are - Net Nanny, WebWatcher, McAfee Safe Eyes, Profil Parental Filter 2, PC Pandora. But there is plenty of free software such as Norton Family, Bitdefender, KuruPiraWebFilter, FortiClient and so on.

Advantages: Depending on the product it may include features as - Website Filtering & Blocking, Social Network Blocking, Instant Message/Chat Blocking, Online Search Filtering, File Transfer Blocking and Application Blocking.

Disadvantages: The initial installation and configuration requires spending time in proportion to the number of users and workstations. Any change in company policy involving a change of information classification, will require reconfiguring of installed programs. This activity could take a long time and expose sensitive data to risk. Additional uncertainty is raised by the possibility that the program could stop working – as a result of a bug in the operating system in the program itself or caused by users' actions. This would allow a free flow of information within the network.

3) Specific router software or firmware

Most popular routers offer some sort of "parental control" or "internet access policy". Often the ability to filter content depends on the brand of router and even its model. For this reason, some administrators choose to use server with Unix-based operating system between users and Internet. This allows the use of specialized software for filtering, with fine tuning of the rules. Some of the examples include:

- pfSense - free, open source customized distribution of FreeBSD tailored for use as a firewall and router [22].
- netfilter.org - software of the packet filtering framework inside the Linux 2.4.x and later kernel series [24].
- DansGuardian - Open Source web content filter which currently runs on Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X, HP-UX, and Solaris [23].

Advantages and features:

- stateless and stateful packet filtering
- all kinds of network address and port translation, e.g. NAT/NAPT (IPv4 and IPv6)
- packet manipulation like altering the TOS/DSCP/ECN bits of the IP header
- filtering the actual content of pages based on many methods including phrase matching, PICS filtering and URL filtering
- Ability to setup and firewall multiple subnets (separate Accounting, Marketing, R&D and sales from each other)
- other

Due to the numerous features, the inability for interference from users and the centralized configuration - this method can be referred to as the best option for preventing leakage of sensitive data so far. However, it does not completely eliminate the possibility of such data misuse. If employees use an encrypted connection, packet filtering becomes impossible (or at least really difficult to apply). To do this the employee has to connect to remote computer via HTTPS protocol which will grant him/her the opportunity to post whatever he/she wants. Another extremely serious problem is the use of VPN or networks for online anonymity like TOR, where the original data, including its destination, are encrypted and re-encrypted multiple times.

4) Software in the Cloud

OpenDNS is a company that provides free DNS servers and basic filtering of visited sites. OpenDNS offers Umbrella - some of the features include: control access to websites depending to the user group, individual user, time of day, IP; VPN; creating black lists and white lists; centralized policy configuration. Despite the user friendly interface and multiple features, the service does offer the ability to filter packets depending on the content.

The disadvantages are similar to listed in C): employees could connect to a remote computer or use VPN. As an additional drawback can be mentioned the fact that part of the security policy is managed by third parties.

5) Facebook

The last line of defense for mitigating the risk of sensitive data disclosure is the Facebook itself. If users have overcome previous controls they may freely publish whatever information they want. One possible solution is assigning employees responsible for information security to check the data published by their colleagues. A serious drawback is not only that it is time consuming activity but also the fact that Facebook offers features for limiting visibility for user’s action. Every employee would certainly limit his supervisor’s access to obscure malicious actions.

Monitoring and filtering employee’s actions in the Internet raises questions concerning the right to personal communication. Considering this fact is vital for defining authorities of the security personnel but should not stop the applying of such controls:

1) Social networks are a source of a variety of attacks that can compromise the security of the organization. This is identified by the majority of security specialists - according to Sophos research [19], to the question „Which social network do you think poses the biggest risk to security?“, 63% of respondents answered: “Facebook”.

2) The workplace is generally not a private place and employees are hired for the purpose of attending to the employers' business, not personal matters [5].

5. Results - Evaluation of existing controls

After analysing the existing controls, we can systematize their advantages and disadvantages in the following table:

Table 1. Results of evaluation of existing controls

	1	2	3	4	5
centralized governance	+	-	+	+	+
filter web sites	+	+	+	+	
filter searches	+	+	+	+	
identify or filter phrases send	+	-	+	-	+
overrun by hacking OS	-	+	-	-	-
overrun with network hack (using remote access with https, TOR-like network etc.)	-	-	+	+	-
Possibility of third party interference	-	-	-	+	+

First four criteria consist mainly of technical specifications relating to the nature of the control. The second half of the criteria relates to the reliability of the control including the possibility of Information leakage to third parties.

From the analysis of the results we came to the following conclusions:

IT security training and awareness is a key control for preventing disclosure of sensitive data. Quality training of employees includes a clear definition of types of information and restrictions on its distribution. This is a prerequisite for achieving self-control from consumers, which creates a secure base for the implementation of disclosure and corrective controls. Unfortunately security policy alone is not enough. It can be ignored either consciously or unconsciously - in case that it is not sufficiently spread to employees.

Installing "parental control" software is ineffective in an organization with many computer stations - centralized control is impossible and the reliability is not high because of the potential shutdown of the application. Creating application software with centralized management to filter information posted by users which is not susceptible to failures in the operating system can be identified as a subject of further research. Such software should be tested carefully for eventual decline in computer performance and employees.

Installation and configuration of specific software in the routers of the organization and use of OpenDNS are alternatives that can be added to the security policy. We found that OpenDNS is less reliable because it does not allow filtering of packets sent based on their content and it actually stores part of the security policy to third party servers.

In case that a user is able to pass all previous controls, he/she could publish confidential information in the social network. To reveal such security breach and prevent a new one, it is necessary to implement control that examines employees’ publications. One of the possible solutions to this problem is monitoring employees’ post by their colleagues that are part of security department. This form of control is not suitable for all needs because employees could use privacy settings for their Facebook profiles and hide information from the monitoring colleagues.

To avoid this disadvantage, we offer an alternative approach - creating a Facebook application. Facebook offers a set of APIs [25] to third party developers. Facebook applications can get access to users’ data and actions. This application can check whether employees’ actions in the social network meet the security policy of the company. The Keyword Insights API exposes an analysis layer on top of all Facebook posts that enable programmers to query aggregate, anonymous insights about users mentioning a certain term [15]. The keywords can be managed in centralized manner. This has the potential to become reliable detective control if it is installed on every employee’s Facebook profile.

6. Conclusion

Facebook shows no signs of weakness in regard to number of users. Furthermore, its growing usage makes more people attracted to the possibility of sharing information. This means that in the near future there will be more employees using Facebook which increases the probability of disclosure of sensitive data. Taking this into account will make countermeasures against information leakage important part of each company's security policy.

We found that the most reliable combination of controls mitigating the risk of leakage of confidential information is:

1. Creating a security policy, distributing it to employees and motivating them to comply.

2. Installing and configuring specialized router software. Centralized management allows making quick changes and does not reduce the performance of client computers.

3. Developing a Facebook application, monitoring the activities of the company's employees who have access to confidential information.

Any combination of controls excluding one of these three cannot provide sufficient reliability and will leave the organization open to information security breach.

The research shows that the creation, implementation and monitoring of the application of a strategy to reduce the risk effect of the use of social networks is crucial to protect the confidentiality of the information. Such strategy is almost always less expensive than repairing damage caused by the risk event. The proposed strategy has the potential to assist organizations and security administrators in the development of system for information security. It can be used by IT auditors in process of assessing the risk (during testing and evaluating the controls) and providing the most appropriate findings and recommendations.

References

[1]. Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic commerce research and applications*, *9*(1), 50-60.

[2]. Silowash, G. J., Cappelli, D. M., Moore, A. P., Trzeciak, R. F., Shimeall, T., & Flynn, L. (2012). Common sense guide to mitigating insider threats.

[3]. J. Barlowa, M. Warkentinb, D. Ormondb, A. Dennisa, (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers &Security, *39* (B),145–159.

[4]. J. D'Arcy, A. Hovav, D. Galletta. (2009), User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, *20*(1), 79–98

[5]. Eivazi, K. (2011). Computer use monitoring and privacy at work. *Computer Law & Security Review*, *27*(5), 516-523.

[6]. Strater, K., & Lipford, H. R. (2008, September). Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1* (pp. 111-119). British Computer Society.

[7]. M. Karjalainen, M. Siponen, (2011).Toward a new meta-theory for designing information systems (IS) security training approaches. Journal of the Association for Information Systems, 12(8), 518–555.

[8]. M. Warkentin, R. Willison,(2009). Behavioral and policy issues in information systems security: the insider threat European Journal of Information Systems, 18(2), 101–105.

[9]. V. Kisekka, S. Bagchi-Sen, H. R. Rao, (2013). Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users. Computers in Human Behavior, 29(6), 2722–2729

[10]. W. Smith, D. Kidder, (2010). You've been tagged! (Then again, maybe not): Employers and Facebook. Business Horizons, 53 (5), 491–499.

[11]. Computer Fraud & Security.(2009), 2009(9), pp. 20.

[12]. Bradbury, D. (2012). Spreading fear on Facebook. *Network Security*, *2012*(10), 15-17.

[13]. Data Use Policy. (2013), Facebook. https://www.facebook.com/about/privacy/your-info (accessed 14.02.2014).

[14]. ISO27k, 2013, Information Classification Policy. (2013). ISO/IEC 27001:2005 A.7.2.1 http://www.iso27001security.com/ISO27k_Model_policy_on_information_classification.pdf (accessed 18.02.2014).

[15]. Keyword Insights, 2013, Keyword Insights. (2013). Facebook. https://developers.facebook.com/docs/keyword_insights/ (accessed 18.02.2014).

[16]. Network Security, News, 2010 (6) (2010), pp. 20.

[17]. Newsroom, 2013, Newsroom. (2013). Facebook. <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22>. (accessed 22.02.2014).

[18]. Parental Software Reviews, 2013, 2014 Best Parental Software Reviews and Comparison.(2013) .TopTenReviews,

http://parental-software-review.toptenreviews.com/ (accessed 23.02.2014).

[19]. Sophos, 2010, Security Threat Report:2010. (2013). Sophos, http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf (accessed 01.03.2014).

[20]. Stanford University, 2013, Data Classification, Access, Transmittal, and Storage. (2013). Stanford University, http://www.stanford.edu/group/security/securecomputing/dataclasschart.html (accessed 01.03.2014).

[21]. University of Michigan, 2013, Institutional Data Resource Management Policy 601.12. (2013). University of Michigan, http://spg.umich.edu/policy/601.12 (accessed 02.03.2014).

[22]. http://www.pfsense.org/ (accessed 03.03.2014).

[23]. http://dansguardian.org/ (accessed 03.03.2014).

[24]. http://www.netfilter.org/ (accessed 03.03.2014).

[25]. https://developers.facebook.com/docs/reference/apis/ (accessed 03.03.2014).

Corresponding author: Ivan Kuyumdzhiev
*Institution:*University of Economics – Varna, Bulgaria
E-mail: ivan_ognyanov@ue-varna.bg