STUDY ON COMPANY SECURITY POLICIES FROM DIGITAL MEDIA

CRISTINA-MARIA RĂDULESCU
PH.D., BABES-BOLYAI UNIVERSITY, FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION,
DEPARTMENT OF ECONOMICS AND INTERNATIONAL AFFAIRS
CLUJ-NAPOCA, ROMANIA
cristinaradulescu2010@yahoo.com

Abstract

The Internet development has brought both new opportunities and risks for either retailers or consumers. For example, electronic commerce is much faster and less expensive, but this openness makes it difficult to secure. People are aware of the fact that online businesses collecting, process and distribute enormous amounts of personal data and therefore, are concerned about their unauthorized use or their use in other purposes than intended by third parties in order to gain unauthorized access to them. There are more examples of cyber criminal activities, such as: hacking, software piracy, passwords attack, service prohibition attacks, scamming, etc. Such fears led to the editing of protection policies meant to secure personal data and to develop some mechanisms to ensure the reliability and confidentiality of electronic information. Security measures include access control devices, installation of firewalls and intrusion detection devices, of some security procedures to identify and authenticate authorized users of network systems. Such mechanisms constitute the core of this study. We will also analyze security and confidentiality policy of personal data of Google Inc.

Keywords: *digital economy, security policies, trust, confidentiality, security mechanisms, cookies, encryption.*

Classification JEL: *F16*

1. Introduction

Trust is the foundation of trade and interpersonal relations (McKnight and Chervany, 2002). Such a condition is vital for distance relationships. People's feeling of helplessness related to the unseen face of the Internet drives their fear of doing business in the virtual environment (Essinger, 2001). Due to the increased complexity of transactions performed by computers, users need for increased confidence is growing obvious.

What is and what does this confidence mean? In the DEX, trust is defined as "feeling of safety coming from one's honesty, good faith or sincerity". Therefore, it is clear that the concept of trust is often associated with certain qualities of the other party, such as honesty, kindness, strength, ability, courtesy, honesty and predictability.

A confident state means the extent to which a person is willing to generally depend on others, given a wide range of people and situations. To depend, means to allow the other to perform something on your behalf, to be deemed reliable and well-intended. For instance, the costumer imagines that the seller will act in favour of his interests, that during the transaction he will prove honesty, competence and readiness to meet its commitment. A person displaying confident attitude will be likely to accept taking some normal risks to buy goods and online services until a bad experience (e.g. a fraudulent credit card) will determine to change the attitude towards online sellers.

People can be born with a confident nature or they can simply develop this feature throughout their lives. The feeling of security reflects the emotional confidence. Researchers found that in new situations, people trust others due to external elements or structures that assure them that things will turn well for them. Thus, people trust each other, not because they personally know one another, but because there are certain conditions of licensing, auditing, laws or bodies exercising coercive force of the state, that ensures that others will be punished in case our rights or interests are threatened or violated (Esen, 2002).

Online dealers try through various actions to prove the safety of their websites (Chang, and Dasgupta, 2015), despite all security shortcomings existing in the virtual environment, in general. Data protection, customer service, links to other sites and warranties, help increase users' trust in the online environment. In

particular, interaction with consumers (Brandt, 2011) will make them believe that the trader is benevolent, competent, honest and predictable and will facilitate the purchase process, is cooperative, ready to share information and have more confidence in the online environment. Links to other well-established sites also have a positive impact on the users' confidence.

2. Mechanisms to ensure security in the digital media

Further we will make a brief presentation of the mechanisms through which is being tried the ensuring of security in online environment.

2.1.Encryption

Encryption is the process of changing the message so as to hide its original content and make it very difficult to read without knowing the corresponding mechanism (the key). Encryption has become an essential technology (Stallings, 2002) in insuring protection of personal and confidential data in an open network (Jay and Hamilton, 2003). On the other hand, decryption is the reversed process, by which encrypted data are brought to their intelligible form. These two processes can be made in two ways:

- private key system(or symmetric algorithms);
- public key system (or asymmetric algorithms).

2.1.1 The Private Key System is the most widely used method of data encryption using a single key both for encrypting and decrypting. Using this system, the sides agree on one key before starting the electronic transaction and it is very important for them to keep confidentiality regarding that key. The two advantages of this system are that it is cost-effective and much faster than the public key system. Among its disadvantages there is the fact that this key must be kept secret, because access to it will make messages become public. Private key unauthorized possessors may decrypt the message and can steal one of the sides' identity by means of sending false information to the other side. Another disadvantage consists in the need for separate keys of each pair of users on the network, fact that brings a significant increase in the number of keys as well as in the number of users, which obviously leads to their difficult management.

2.1.2 The Public Key System

Public key encryption uses a double-key algorithm with two different but mathematically associated keys – private and public. The private key must be kept secret and be recognized only by the rightful possessor. It must be made public, but associated with a certain possessor.

The advantage of this system is that it eliminates the key exchange specific to the private key system. The disadvantage consists in a difficult usage of the computing power required by this type of encryption which makes it less practical. Moreover, the public key systems are vulnerable to attacks with normal selected text and they are a bit expensive in usage.

In practice, a combination between private and public key systems is used to insure the guarantee of data confidentiality, because only the user's public can decrypt the secret key which in its turn is necessary for actual decrypting of the message.

2.2. Electronic certificates

An electronic certificate is a document that usually contains a public key, the key holder's name and a digital signature (Murray, 2003) to authenticate the whole package. The main purpose of an electronic certificate is to confirm that the information on the certificate has been verified and certified as true and credible elsewhere. This may include the following: the sender's and the public key holder's name, the certificate expiry date, the serial number, etc.

2.3 Access control to systems

Organizations involved in electronic marketing can insure protection confidentiality of electronic information from unauthorized access using identification numbers and user passwords.

2.4. Intrusion detection

Although, generally considered that the outside world represents the greatest threat for online security, statistics show that a large percentage of intrusions come from organizations. The faster an intrusion is detected, the faster an attacker can be identified and removed from the system before producing substantial damage (Lo, 2003).

2.5. Protection walls (firewalls)

A firewall is a device that prevents unauthorized users from accessing the system's network marketers (Hazari, 2000). Its implementation requires a certain level of experience. Hazari stated that: "we can think of firewalls as something similar to a nightclub guard. As a guard…the wall has a set of rules, similar to the guest list or a dress code that determine the data that should enter the system. Just like a guard posted at the club entrance, the wall is located at the entry point where the internet data are trying to enter your computer."

2.6. Secure Electronic Transactions (SET)

Represents a security protocol that uses digital certificates and signatures to insure transactions, allowing parties in a transaction to confirm each other's identity (Chaffey, 2002). SET is incorporated into several payment options such as smart cards, digital cash and electronic checks in order to better secure payment systems and provides three key services (Gay, Charlesworth and Esen, 2007):

- a secure communication channel between the parties involved in a transaction;
- improved reliability by means of digital certificates and digital signatures;
- insured confidentiality by providing only relevant information to parties.

3. Mechanisms for ensuring privacy in the digital media

The European Directive on privacy and electronic communications from 2002[1], aimed at protecting the fundamental rights and individuals, in terms of their personal information confidentiality. It offered new rules on confidentiality, security, data retention, use of cookies, spams, data traffic/ locations etc. The basic idea is this: any organization that collects, processes and stores personal individual data must follow some basic principles such as fair data processing only for the purpose they were collected, data accuracy, updating kept only as long as necessary, proper security and data transfer to countries not belonging to the European Economic Area, except for those which ensure adequate data protection means[2].

Therefore, any person whose data have been processed has the right to access his personal data, to request correction, updating or deletion of holder's records[3].

4. Consideration on Google security policy

4.1. General information about Google

Google Inc. is a US multinational corporation founded in 1998 by Larry Page and Sergey Brin, PhD at Stanford University, and provides a simple and quick method of finding information on the Web, with a database of over 8 billion web sites[4]. Its service offer include among others Internet search engines – Google, Google Earth, which provide satellite images of Earth, the Google Chrome browser, the open source operating system for mobile devices – Android, the e-mail – Gmail, Google Talk – instant messaging, Google Chrome OS operating system based on Linux kernel, Orkut and Google+ social networks, etc.

Google has the ability to track users interests in affiliated sites by using the "double click" and Analytics technologies. Google AdWords service allows advertisers to automatically show ads on the web based on information search results through Google engine[5]. Owners of sites like Google can display AdSense ads on their site and have the right to charge money for every ad viewed. In 2011, 96% of Google's revenue came from advertising.

4.2. Security measures

Google puts considerable efforts into protecting the users against unauthorized access or alteration, unauthorized disclosure or destruction of information it holds. In this respect, it adopted the following measures:

- SSL encryption using multiple services;
- Provision of two-step verification methods when accessing Google Account and Safe Browsing functions in Google Chrome;
- Revision of information collection, storage and processing, including physical security measures to protect against unauthorized access to systems;
- Restriction of access to personal information, given only to Google staff, contractors and agents who are entitled to find this information to be able to process them on behalf of the company and subject to strict contractual confidentiality obligations.

5. Consideration on Google privacy policy

5.1. Google data processing

Google processes information based on their clients' search activity on the site[6] and the applications used by them, information such as the spoken language, watched videos, searched places on Google Earth, their IDs device, IP addresses, data regarding cookies and visited destinations, things they like and people who drive the customers' greatest interest.

A cookie is a small piece of text in the browser created by the website that a person accesses. By its help, the website retains information about one's visits, for example, preferred language and other settings. In this way, further visits can be made much simpler and the site turns more useful. Cookies play an important role. Without them, using the Internet would be a more unfriendly experience. Google uses cookies for various purposes. For instance, to retain the customer's navigation preferences, to offer more relevant ads, counting users accessing a page, for customer data protection, etc.

5.2. Purposes of data processing described in Google policy

The reasons for which the company collects and processes customer data are:

- to help the company offer more relevant search results, a more useful and personalized content;
- to provide ads based on customer interests, taking into account the searches or watched videos on YouTube;
- to improve security by means of anti-fraud and abuse protective measures;
- to carry out statistics and measurements.

5.3. Customer privacy protection solutions

Customers can set how Google uses personal information. They can disable interests and can learn how to manage cookies. YouTube viewing history or search history, can opt out of displaying ads based on interests and can learn how to manage cookies[7].

Google obliges to provide its customers access to personal information. If the information proves to be incorrect, customers can demand for rapid updating or deletion provided the information must be kept for legitimate business purposes or legal cases and circumstances where requests are unreasonably repeated requiring an excessive technical effort (for example, developing a new system or the structural changing an existing practice), which might violate others' privacy or would be extremely impractical.

Google's Privacy Policy applies to all services offered by Google Inc. and its affiliates, including YouTube, Google services on Android devices and on other sites (such as advertising services), but excludes services that have separate privacy policies which have excluded this Privacy Policy.

6. Conclusions

The conclusion that can be drawn from this study is that insurance of security techniques and confidentiality policies on online corporate customers are multiple and have become more bulky. Given the growing concerns of customers and existing strong arguments in the literature, big companies like Google and

others have been forced to comply with legal and customer requirements. I believe, however, that the present topic is still a very sensitive one and holds many unknown aspects to the vast majority of users. Even if companies have proceeded to pass a set of rules on security protection and confidentiality, in reality it is the highly specialized language that could raise problems including the bodies called upon to settle any disputes related to the de facto compliance of these rules.

[1]*(It's about the Directive 2002/58 / EC of the European Parliament and of the European Council of 12 July 2002 concerning personal data processing and privacy protection in the digital communications sector (Directive on privacy and electronic communications)).*
[2]*(If a host country does not have the appropriate level of protection, it must comply with one of the following: data subjects have agreed to the terms, the transfer is required by law, the transfer is made to establish a contract with the data subject or on behalf of the data holder, transfer is necessary for obtaining legal advice or for the prevention of injury or great damage; data is an abstract from a public status register).*
[3]*(In Romanian Law there is law no. 677 of 21 November 2001, amended and supplemented, regarding the protection of individuals with regard to personal data processing and the their free movement).*
[4]*(At the end of 2007 it was ranked to be the strongest global brand, based on criteria such as value in millions dollars ($ 86,057,000 US), and by users perception).*
[5]*(Issue 1/2012 of the prestigious German news magazine "Der Spiegel" published an article about Google titled "Fishermen in the ocean of data" on January 2. 2012. The subtitle was: "Google determines what is important and what is not in this world", referring to the manner and order in which the Google search engine displays its search results).*
[6]*(And other companies have done and do likewise. In 1999, Amazon bought a small online service called PlanetAll which, based on book sales, identifies people's postal codes and e-mail addresses. Amazon has used this information to recommend books to people with similar tastes and preferences identified by the system. In a speech from 1998, Jeff Bezos, the company president stated: "What we can do is to use advanced technologies like collaborative filtering and others to speed up the discovery process. Therefore, if today you have a chance of 1:1,000 to come across a book to be hooked by the moment you walk into a bookstore, we want to use technology to be able to know you in person and increase the odds to 1:300. Then to 1:100. And then, in several years of work to get to a 1:50 chance and so on. It is something that the world will highly appreciate. Great traders have not ever had the chance to know their customers in a truly personal manner. Electronic commerce will make this possible."Throughout its way, the company had to change this practice, offering buyers an option not to be included in the information share program).*
[7]*(More information on this can be acquired via www.google.com/policies. Additionally, customers can manage their data privacy options using myaccount.google.com).*

7. Bibliography

[1]Brice W.*"Electronic signatures in the real world"*, www.messageg.com/security/brice/html;
[2]Chaffey D. [2002], "*E-Business and E-Commerce Management"*, 457, 459, PrenticeHali;
[3] D. Harrison McKnight and Norman L. Chervany, [2002] *"What Trust Means in E-Commerce Customer Relationships: An InterdisciplinaryConceptualTypology "*, International Journal of Electronic Commerce, vol. 6, no. 2, p. 35-59 ;
[4]Esen R. [2002] *"Cyber crime: agrowingproblem",* The Journal of Criminal Law, 66(3), 269 – whereshehighlightsthat the lawlessness on the Internet may lead to lake of trust on the part of consumers;
[5]Essinger J. [2001] *"Internet Trust and Security",* Addison-Wesley;
[6]Hazari S. [2000], *"Firewalls for beginners",*www.securityfocus.com/focus/basics/articles/fwbeg.htm;
[7]Jeffrey Chang, BarunDasgupta, *"An investigation of the barriers to E-business implementation in small and medium-sized enterprieses"*, [2015], International Journal of Social, Behavioral, Economic and Management Engeneering, vol. 9, no. 1, p. 26-36;
[8] Jay R. & Hamilton A. [2003] *"Data Protection: Law&Practice",* Sweet and Maxwell;
[9] Lo J. [2003] "*Denial of Service or "Nuke' Attacks"*, www.irchelp.org/irchelp/security;
[10] Murray J, [2003] *"Public key infrastructure digital signature and sistematic risk"* JILT Vol. 1;
[11] Richard L. Brandt,[2011] "*One click – Jeff Bezos and the rise of Amazon.com",*Portofolio Penguin;
[12] Richard Gay, Alan Charlesworth, Rita Esen [2007], *"Marketing on-line – A Customer-Led Approach"*, Oxford University Press;
[13] Stallings W. [2002] *"Introduction to Secure Electronic Transaction (SET)*", www.informit.com;

[14] www.google.com/policies;
[15] https://ro.wikipedia.org/wiki/Google;
[16] http://www.amazon.com/dp/B005MJFA9K/ref=rdr_kindle_ext_tmb.