IBIMA Publishing
Communications of the IBIMA
http://www.ibimapublishing.com/journals/CIBIMA/cibima.html
Vol. 2011 (2011), Article ID 130212, 15 pages
DOI: 10.5171/2011.130212

Information and Communications Technology Threats: Personal Data and User Behaviour

Daniel Lang[1] and Jean-Luc Pillet[2]

[1]TELECOM Ecole de Management, Institut TELECOM, France

[2]HEC Genève, Genève

Abstract

This article analyses the threats which Information and Communications Technologies currently pose to individual liberties. Indeed, the information which is collected on individuals is becoming more and more complex: via RFID chips inserted into different cards (including transport, bank and customer loyalty cards), via visits to internet sites, over surveillance cameras posted in various places (work and public spaces), each of us is leaving « traces » which make up just as much collected data, most often treated and transmitted without our knowledge, and integrated into files, the mastery of which eludes us. We wished to carry out a study in order to evaluate the use of information and communications technologies and the awareness of users to the inherent risks. We also sought to determine if there exists a significant gap between the awareness of a threat and the safety measures associated in order to reduce the vulnerability of a system.

Key words: Threat, Information and Communications Technology, individual liberties

Introduction

Information and Communication Technologies and «Big Brother »

In recent years, technological evolutions have considerably modified how companies communicate. In 1989, management at the multinational Eli Lilly, precursor in the subject, discretely offered its employees the possibility of being connected to an internal message system in the company (around 30'000 collaborators) in order to be reached even during the weekend. This request did not remain isolated. Very rapidly, the professional world adapted to a way of being permanently connected and today it is an even larger population that is conforming to this practice of always being connected. Independent consultants, nomad workers, high school students, domestic workers: many have adopted the Pavlovian reflex which consists in turning on the mobile, notebook or Smartphone on a daily basis and transferring personal data over various channels: SMS, instant messaging and email. The number of communication tools using Wi-fi networks, 3G or cables has allowed the transfer of video images and documents which can be stored and thus made visible on Internet sites to a considerable number of Internet users.

We are discovering thus that, current technology is allowing tracking individuals in their comings and goings (GPS on a mobile), visualising their silhouettes thanks to Google Street View in a listed street, watching their daily tasks in a workplace with camera surveillance, and storing their personal data with a third party whose actual level of security is not known Piatti, M.C. (2001). Information and Communications Technologies thus, ensure the tracking of objects and individuals. On a daily basis, numerous information systems memorise our activities, purchases, centres of interest, exchanged messages... All of this information that is collected by various organisations once centralised, allows the creation of a profile for each individual. From now on, many larger companies will categorise their cliental according to different groups (for example; Gold, Silver, Bronze, Zapper) in order to adapt their marketing tactics to the consumer profile.

All of these tools; Internet, mobile phones, diverse administrative computer files, various cards (identity cards, payment cards, transport cards, loyalty cards, professional badges...) and RFID tags placed in certain objects, can lead to certain excesses and represent a real threat to the respect of private life and individual liberties. To be noted are three significant threats unleashed by Information and Communication Technologies:

Tracking Individuals

One of the first abuses of RFID systems could very well be the geolocation of individuals. In fact, some of these tools offer the possibility of placing and following individuals' movements in public spaces such as stations, airports, shopping centres,... and soon anywhere in the world Hermitte, M.A. (2003), Ta, C.D (2004).

In the line of RFID tags, implanted chips allow the tracking of animals, but also the identification and the localisation of individuals by satellite. In fact, an electronic chip in the size of a grain of rice can be implanted under the skin of an individual in order to memorise biological information (heart rhythm, current medical treatment...) or to register personal data in the place of an identity or payment card. Some American hospitals offer their patients the possibility of chip implants containing their medical files in the hopes of avoiding any errors in treatments. The implants make medical surveillance from a distance possible by automatically sending an alert to specialised care units Mattéi J-F. (2003).

For that matter, mobile phones, even in sleep mode, make it possible to localise the holder. In fact, each mobile phone emits a signal at a regular interval that allows the nearest station to identify it and thus transmit calls, messages and SMS. It is in fact indispensable for the telecom operator to localise the subscriber in order to determine the local station that will transmit the call Pedrot P. (2003).

Another technology especially used by certain States to track crime: video surveillance. The number of cameras, in public spaces as well as work spaces (warehouses, factories...) is growing rapidly in order to control all sorts of activities or suspicious behaviour. Thanks to facial recognition software, it is now possible to recognise the portrait of an individual out of a crowd filmed by a video surveillance camera linked to an information system. The surveillance process can thus be automated to localise a wanted person. Moreover, with the spread of biometric identity cards, it will be easy to track the movements of an individual in a town equipped with video surveillance systems. Certain companies are integrating these systems into their warehouses and/or depots in order to see the crimes and thefts committed by certain employees.

Profiling

Another case of the attractive use of RFID tags for companies stems from their information storage capacities. In fact, the entirety of information collected by one tag can become very useful to a company to define the client's profile. RFID tags can in fact offer a great deal of information which is difficult for companies to access and which complements their client database.

They thus have access to our behaviour, our choices, our preferences...Agre, P.E. and Rottenberg, M. (1998). The use of this information for commercial gain remains nevertheless a violation of one's private life.
We will attempt to identify the uses and risks associated with these various tools. In fact, by linking a customer loyalty card with a payment card for an individual, his or her expenses, consumption, travel, tastes (culinary, cultural...) are memorised by the actors of large distribution in order to
determine the profile of a particular client Gearthy, C. (2006). In order to optimise the management of stocks, supplies and better target promotional activities, the information systems of the large distributors record the products purchased by each client through gigantic Data Warehouses Kimball, R. and Ross, M. (2003), Tufféry, S. (2007). The files in public and private organisations contain much personal data on thousands, even millions of individuals. This randomly collected data remains inoffensive as long as it is memorised in a distributive manner. However, a certain number of companies are specialised in the collection of personal information for commercial ends Poullet, Y. and Rouvroy, A. (2007).

Internet users leave numerous traces on their computers of Web sites they have consulted and personal information they have left during their visits. This information, registered in files (entitled cookies) is remotely accessible and thus allows the Web sites to identify users and draw up their profile.

Finally, to complete this panorama of the tracking of objects and individuals, the electronic wallet memorizes information on the identity of the holder and his or her purchases, on the Internet as well as in certain physical points of sale. This new means of payment makes it possible to track the movement and the purchases of an individual.

New Excesses Linked to Personal Data

Even if the potential of Information and Communication Technologies in terms of profitability and practicality is very attractive, the disappointments are numerous. In French Switzerland, a few months ago, a doctor lost all of the data of his patients, which was contained in his portable computer which was stolen from his car. The impact is important since it affects the follow-up of his patients but also confidential information which could be known by unscrupulous individuals. Another case, in France: a police officer sold photos of the fugitive Jean-Pierre Tréber that were filmed by a surveillance camera to the Figaro (Rizet, Zemouri, 2009). We see here that sensitive information is also up for sale and points directly to an error on the part of the administration. Other numerous examples can be cited by (Ghernaouti-Helie, 2009).

With the use of Internet in the professional world, Human Resources can also pick up on compromising photos often posted by "good" friends of the potential candidate. An apprentice thus lost his job after a photo of him at a party with alcohol was visualized. The approach can also be subtler. An employee on sick leave was punished because she was using the Internet at home. The use of Internet was incompatible with the type of sickness she had declared.

As a general rule, in a company, employees can make known confidential information without really realising the value of the broadcasted information Martin, A. (2008). In fact, a simple look at social networking sites where Internet users divulge seemingly anodyne information can have a certain value for economic actors. How do we know that an unfair competitor will never use information on Curriculum Vitae? We have already heard about the cases where company X offered a fictitious similar job to a future candidate in order to make him talk about his experiences in company Y.

Another example, on 24 march 2010, a young French hacker got hold of administrative rights on Twitter and was thus able to consult internal documents of the company. The collaborators at Zataz.com met with the young hacker to better estimate the type of information he was holding: "I will not say anything, for the moment. Just that I have, for example, the dietary restrictions of certain employees, the access codes to the Twitter office for each employee: the detailed telephone communications records of Evan Williams [the head of Twitter, NDR], ... and I know exactly what the employees said after my break-in. For example, Jason Goldman warned, the same day, all of the employees".

Attempts for a Better Framework

Politicians facing these excesses are attempting to better frame the Web. Two senators, Yves Détraigne and Anne-Marie Escoffier, have proposed a law that would allow the right to forget Larchet, S. (2010). In a domain which differs little from the localisation of sites and streets where cars and people can be identified (Google Street View), the PFPDT ("Préposé fédéral à la protection des données et à la transparence") considers that it consists of data of a private nature, is taking the case to court and is asking Google to immediately take down its « Google Street View » software from Swiss territory. Google initially rejected this demand but an agreement was reached with the multinational on 21 December 2009. Thus " Google commits to no longer publishing on Internet any new images taken in Switzerland for Street View, neither in the context of its online service Street View, nor in the context of any other of its products, and this until the Federal Administrative Tribunal has given its ruling and the decision be enforced". In France, the CNIL is also proposing recommendations concerning the protection of data Féral-schuhl, C. (2002).

In Switzerland, in order to avoid the abuse of surveillance cameras in the workplace, the OLT labour law (*l'ordonnance sur la loi du travail*) stipulates in article 26 : « (1) It is forbidden to use systems of surveillance or control designed for the surveillance of the behaviour of workers at their work space. (2) When systems of surveillance or control are necessary for other reasons, they must be designed and arranged in a manner to not affect the health and the freedom of movement of workers. ». It is a question of respecting the general principles of proportion, transparency and purpose.

Current limitations

Nevertheless, in spite of the drafting of legal rules to put a stop to the lack of delicacy and offense, both are subject only to the jurisdiction of a country. It is extremely difficult to shut down a dubious Web site beyond the borders of the legal dispute. In France, the government is aware of the international dimension to the problem as Internet goes beyond geographical borders. "The closure of an illicit site in one country can result in its being immediately hosted in another. It is a useless waste of energy and inefficient for the protection of our citizens" (Guerrier, 2008). In fact, by its very nature, the Internet is planetary. Nevertheless, even if some dream of a technological space "without laws", it is the opposite which is occurring. Each state has its own jurisdiction and it is necessary to take into account the local jurisdiction where an individual is trampled upon - which makes this all rather complicated!

From a technical and organisational point of view Foray, B. (2007), security officers and other information administrators must face the lively imagination of hackers in order to avoid the theft of data. (Bloch, Wolfhugel, 2007), (Maiwald, 2004) by explaining the principles and methods. The following schema Shimeall, T. (2002) shows the evolution of diverse techniques used by information thieves:

When looking more specifically at the attacks related to data protection, one may cite the following:

- *Spyware* : software which transmits private information
- *Viruses and malwares* : stealing passwords on the hard drive and intercepting passwords in the browser and on the keyboard

- *Worms* : autonomous programmes that can be found on the hard drive

- *Hoaxes* : false information of a catastrophic nature

- *Jokes* : funny programmes that one sends to friends

- *Backdoors* : system, screen and keyboard spying

- *Rootkits* : modifies the operating system in order to hide the presence of a file and keys registry

- *Social engineering* : uses the kindness and the innocence of collaborators in order to obtain a maximum amount of information by pretending to be someone else Mitnick, K. (2003)

Thus, regarding the various threats that weigh on the infallible protection of personal data, one can only question the respect of his or her fundamental rights concerning private life, family, residence and correspondence.

The Purpose of Our Research

Voluntarily, the framework of our research focused on general everyday users, those persons who have not been trained to apply the basic security principles of a company. One may cite the standards ISO 27001, ISO 27002, ISO 27005, and the methods for applying them (EBIOS, MEHARI). Theoretical contributions have made it possible to validate these practices within companies: security policies (Schaurette, 2001), agreements on non-disc losure (Peltier, 2000), security training (Siponen, 2000), making users aware (Fites et Kratz, 1993). For an untrained individual in security, the risk management equation takes into consideration 2 fundamental parameters: the impact of probability X is thus only very subjective. In fact, the very notion of probability is of an uncertain character, thus an applicable threat for others. Awareness and behaviour can be strongly dissociated. In a company on the contrary, security administrators strive to obtain a behaviour which is strongly related to security awareness. More generally, it may be noted that certain studies have allowed the creation of a new field of research : factors of influence on security behaviour, (Bergeron, Latour, Pérès, 2003), theory of reasoned action (Fishbein et Aizen, 1967, 1975, 1979, 1980) and attitude measurements (Ostrom, 1969) and (Béland, 1993).

Within the context of our study, we carried out a survey of a specific section of individuals who were "tapped into technologically" and in training in order to find out how they use Information and Communication Technology in general and more specifically the Internet. Our contribution is to show the degree of Internet use among these individuals, and to determine the existence of a security culture associated with acceptable behaviour. Concerning certain aspects of information systems security, we are also seeking to determine if a significant gap exists between awareness of a threat and the associated security behaviour in order to reduce the vulnerability of a system.

The objective of this survey, which we carried out in 2010, is to evaluate the conscience of users with regards to risks linked to the availability of personal data via ITC (and notably on the Internet). It consisted in analysing their awareness of the dangers posed by ITC and studying the security measures taken as a result by the users. We thus, wanted to measure the degree of awareness of risks linked to ITC and to apprehend the impact on the users' practices.

The data used in this exploratory research was collected in the form of a questionnaire sent to 67 students in a French business school. This sample of individuals, members of Generation Y, and familiar with technological tools seemed representative to us in our realization of this analysis.

Our questionnaire was designed around the following themes:

- The degree of Internet usage among our respondents

- The security culture of our respondents

- The security behaviour of our respondents

The questionnaire contained only closed answers, formulated in terms of an attitude scale (a Lickert scale of 5 points). The goal was to find out about the users' awareness of the dangers linked to ITC and the impact on their behaviours. In order to evaluate the risks linked to the use of ITC, several questionnaire items were directed to the perception that the users had of inherent dangers linked to the use of ITC. In order to estimate the security behaviour of users, their practices with regards to the dissemination of personal data was the object of several questions.

Results

With this end in view, our questionnaire consisted of questions linked to the use of Internet and the culture of the candidate specifically linked to the domain of information security. Other questions are relevant to the protection of Internet users. For certain questions, only one answer was possible. For others, it was possible to answer positively to several questions. Here are the answers corresponding to a sample of 67 individuals:

Table 1.a: Responses to the First Part of Our Survey (*Global Results)*

N°	Wording	answer1		answer2		answer3		answer4		answer5	
1	**According to you, a password should include a minimum of how many numbers/letters?**	**5**	4 characters	**21**	6 characters	**32**	8 characters	**5**	10 characters	**4**	12 characters
2	**Do you think that Web sites are the object of attacks by Hackers, on average, once per :**	**31**	week	**21**	month	**5**	semester	**4**	year	**3**	very rarely
3	**Do you think that ICT (PDA, social networks, RFID tags) can pose a threat to your individual liberty?**	**4**	very important	**15**	important	**27**	some	**12**	weak	**2**	it's not a threat
4	**Do you think that Web sites are in general :**	**2**	very secure	**11**	well secured	**32**	correctly secured	**18**	weakly secured	**3**	very little secured
5	**Do you think that the encryption of confidential data (ex. Credit Card numbers) on the Web is :**	**56**	absolutely necessary	**8**	often necessary	**3**	necessary in general	**0**	rarely necessary	**0**	useless
6	**You change your password :**	**0**	weekly	**3**	monthly	**5**	every semester	**6**	yearly	**52**	very rarely
7	**You periodically buy products on e-commerce sites, on average once every :**	**0**	day	**5**	week	**33**	month	**24**	year	**5**	never
8	**Which social networks do you use:**	**60**	Facebook	**4**	Twitter	**7**	LinkedIn	**13**	Viadeo	**8**	other
9	**How often do you use these social network sites :**	**29**	several times/day	**23**	once/day	**10**	once/week	**1**	once/month	**1**	never
10	**What information would you not want to be communicated on a Web page form :**	**42**	your address	**50**	your telephone number	**24**	your photo	**22**	your preferences	**57**	your bank references

Table 1.b: Responses to the Second Part of Our Survey

	Wording	**answer1**		**answer2**		**answer3**		**answer4**		**answer5**	
11	**Before buying a product on the Web, you check :**	**55**	reliability of site (certified)	**43**	encryption of CC N°	**36**	price of products offered	**14**	the SAV	**2**	the number of hacker attacks the site has already received
12	**According to you, which formats for attatched documents can be infected with a virus?**	**56**	.exe	**30**	.jpg	**47**	zip file	**32**	.doc	**13**	.pdf
13	**An authentication corresponds to :**	**22**	who is who?	**43**	who can have access?	**13**	who can see it?	**14**	who can modify it?	**9**	who made it?
14	**A strong authentication corresponds to :**	**7**	what the entity knows	**2**	something you possess	**9**	something you are	**18**	something you know and possess	**16**	something you are and something you have
15	**Do you know the methods used which allow for authentication?**	**25**	One-Time Password (OTP) algorithms	**22**	PKI (Public Key Certificates)	**6**	SMS based on OTP	**21**	finger venous network biometrics	**1**	Match on Card
16	**Most online service providers of online sales inform you contractually of :**	**5**	the inability of maintaining confidential data	**27**	the anonymous use of your data	**18**	the use of cookies	**23**	the sharing of your consolidated data with partners	**39**	the guarantee of keeping your data private
17	**Your data is encrypted on a server in a secure local. How do you estimate this protection?**	**1**	infallible	**25**	there is a residual risk	**35**	there is a risk to consider	**3**	the protection is insufficient	**0**	very insufficient
18	**According to you, hackers are capable of :**	**38**	memorizing your password on the keyboard	**53**	putting up a pirate site which looks like a known site	**26**	using botnets to attack a target	**31**	stealing cookies	**26**	SQL injection requests using a URL
19	**You install anti-virus software on your PC and you notice that it is often running. The protection is ?**	**0**	100% sure	**34**	sure if it is combined with a firewall	**25**	not sure 100% as it cannot protect in real time	**6**	non because an anti-virus can be a fake	**2**	no because an anti-virus can by spyware
20	**You receive an electronic message from your bank where they ask you to transmit your password :**	**40**	you don't answer	**43**	you inform your bank	**1**	you send your password by email				

The Nature and the Links between Various Questions in the Survey

As we stated in point 5, there is a distinction between the questions concerning the use of Internet, the awareness of its potential dangers and the security measures taken by the ICT user. We can schematize the steps in our evaluation in the following manner:

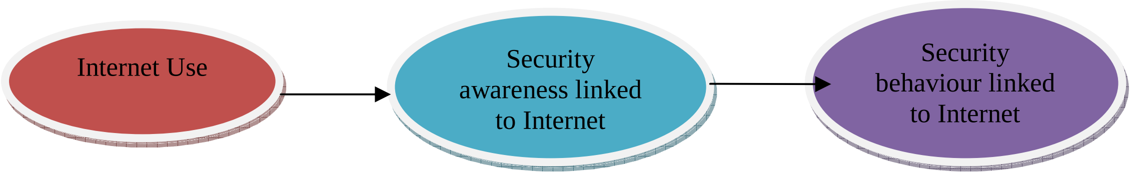
Internet Use
Security awareness linked to Internet
Security behaviour linked to Internet

Figure 1: Determining Indicators of Use, Awareness and Behaviour

There also exists a link between certain questions on a same theme that could allow the measurement of gaps between awareness and security behaviour. The tables below illustrate our approach:

Indicators Used In the Survey Questions

Certain questions only aim at obtaining information concerning practiced uses of the Internet. Other questions validate or not the choice of our respondents as some of the wrong answers show their ignorance of the domain. This evaluation allows us to establish a diagnostic concerning the awareness and the "acceptable" security behaviours of our candidates. The following table classifies the questions according to the concept mentioned in figure 1.

Table 2: Indicators Linked to Survey Questions

Degree of Internet use of our respondents	Security awareness culture of our respondents	Security behaviour of our respondents
N°7, N°8, N°9	N°1, N°2, N°3, N°4, N°5, N°10 N°12, N°13, N°14, N°16, N°18	N°6, N°11, N°17, N°19, N°20, N°15

The following table below makes it possible to show the answers in percentage points and to distinguish independently from Table 2 :

Table 3: The Respondents in % Points with the Evaluation of the Answers

N° question	*Answer1*	*Answer2*	*Answer3*	*Answer4*	*Answer5*
1	🟥 7%	🟥 31%	🟩 48%	🟩 7%	🟩 6%
2	🟩 46%	🟢 31%	🟥 7%	🟥 6%	🟥 4%
3	🟢 6%	🟩 22%	🟩 40%	🟥 18%	🟥 3%
4	▨ 3%	▨ 16%	▨ 50%	▨ 27%	▨ 4%
5	🟩 88%	🟥 13%	🟥 5%	🟥 0%	🟥 0%
6	▨ 0%	🟩 4%	🟢 7%	🟥 9%	🟥 78%
7	▨ 0%	▨ 7%	▨ 49%	▨ 36%	▨ 7%
8	▨ 90%	▨ 6%	▨ 10%	▨ 19%	▨ 12%
9	▨ 43%	▨ 34%	▨ 15%	▨ 1%	▨ 1%
10	🟥 63%	🟢 75%	▨ 36%	▨ 33%	🟥 85%
11	🟩 82%	🟩 64%	▨ 54%	▨ 21%	▨ 3%
12	🟩 84%	🟥 45%	🟩 70%	🟩 48%	🟥 19%
13	🟩 33%	🟥 64%	🟥 19%	🟥 21%	🟥 13%
14	🟥 10%	🟥 3%	🟢 13%	🟩 27%	🟩 24%
15	▨ 37%	▨ 33%	▨ 9%	▨ 31%	▨ 1%
16	🟩 7%	🟩 40%	🟩 27%	🟩 34%	🟥 58%
17	🟥 1%	🟩 37%	🟢 52%	🟥 4%	🟥 0%
18	▨ 57%	▨ 79%	▨ 39%	▨ 46%	▨ 39%
19	🟥 0%	🟢 51%	🟩 37%	🟩 9%	🟩 3%
20	🟢 60%	🟩 64%	🟥 1%		

- Answers of an informational nature ▨
- Acceptable or correct answers 🟢
- The best answer 🟩
- Incorrect answers 🟥

Possible links between a users' awareness of a danger and his or her associated behaviour in order to reduce the risk

Table 4: The Links between Variables of Awareness and Behaviour

The security awareness of a user	and his/her behaviour
Passwords N°1: according to you, a password should contain how many numbers and letters :	*The protection of a « system »* N°6: change your password once every: answers 1 to 5
Information necessary to make an online payment N°10: what information would you not want communicated on a form on the Web?	*Web transactions* N°11: answer 1 : the reliability of the site (certified)
The encrypting of confidential data N°5: the necessity to encrypt confidential data:	*The verification of the encrypting of confidential data* N°11: before buying a product on the Web, do you check : answers 1 and 2
The notion of authentication N°13: an authentication corresponds to : N°14: a strong authentication corresponds :	*The methods of authentication used* N°15: do you know the methods used in authentication, answers 1 to 5
The threat of ICT to individual liberties N°3: Do you think that ICT (PDA, social networks, RFID tags) can pose a threat to your freedom?	*The use of social networks* N°7: which social networks do you use? answers 1 to 5 N°9 : with what frequency do you use these social networks, answers 1 to 5
Binding clauses concerning the protection of data N°16: most online sellers inform you contractually :	*User data on a server in a distant location* N°17: your data is encrypted in a server in a secure location. How do you estimate this protection?

Justifying Good and Less Good Answers

Managing Passwords

A file containing the passwords of users on a server must always be encrypted. One of the possibilities consists of using the Hash function which makes it possible to obtain a condensed version of the password. However, the danger is not completely avoided. In fact, cracking software can generate Hashes that can be compared to those stored in the file "Password" from dictionaries and combinations of alphanumerical characters.

Our Internet Users' Answers

Question N°1: 41 answers (answer 3 + answer 4 + answer 5) out of a total of 67 (61% of Internet users) are correct since a password must be comprised of a minimum of 8 characters. Moreover, certain Web sites oblige Internet users to comply with this restriction. However, the behaviour of a large number of users with regards to changing passwords is not acceptable since question N°6 shows that 8 respondents (answer 0 and 1) out of a total of 64 (13%) change their password each semester. In a company, a responsible information security policy would require putting into place valid password expirations! Microsoft's recommendations on the subject are even more restrictive as they indicate an average duration of 42 days (Microsoft Security Products for Business).

Information Necessary for Online Payments

Question N°10 underlines Internet users' reluctance to give their bank references (57 respondents), their telephone (50 respondents) and their address (42 respondents), successively for a total of 67 respondents in percentage points 85%, 75% and 63%. The answers 3 and 4 of N°10, concerning photos and tastes, are less significant since they seem to affect à minority of our respondents. However, the fear is considerable concerning answers 1, 2 and 5. Their associated behaviour is given by 55 respondents which check the reliability of the site: 82% of the 67 individuals in question N°11, answer 1.

Encrypting Confidential Data

A large majority of respondents consider that the encrypting of confidential data is absolutely necessary (N°5, answer 1) with 56 out of a total of 67, or 84% of answers. The behaviour of our Internet users is not surprising: in question N°11, 55 check the reliability of the site (answer 1) and 43 check the encrypting of the N° of the credit card (answer 2), or 82% and 64% of respondents successively. Answer 2 is the most significant regarding the encrypting of confidential data.

Authentication

The notion of authentication is clarified with regards to other fundamental criteria which define the principles of security in terms of capacity Ghernaouti-Helie, S. (2000): confidentiality, availability traceability and non-rejection

The question "Who is who" makes it possible to answer to the criteria of authentication. It gives proof that the individual really is who he or she claims to be. Different factors allow authentication: it is possible to distinguish what one knows (password), what one possesses (a token) and what one is (biometrics). The authenticators (token) « One-time Password (OTP) » use passwords that change every minute. Certain authenticators can also use digital certificates (Public Key Certificates or PKI) based on the possession of a secret key (RSA). Other methods use the SMS with a code that makes it possible to complete a banking transaction on the Web. A strong authentication is the result of the culmination of a number of factors together. For example, « Match On Card » technology uses biometric prints (what I am) combined with a chip car (what I have).

The answers given by our Internet users seem to show gaps right down to the understanding of the notion of authentication. For question N°13, only 22 individuals checked the correct answer (answer 1), or 33% of respondents. For question N°14 concerning the definition of a strong authentication, we are markedly in a similar bracket: 18 and16 individuals successively for the answer 4 and 5, or 27% and 24% of the total sample. Finally, the use of different methods relative to question N°15 confirms not only the weakness in the awareness of the domain but also its use. Numerous respondents check that the sites are certified and that there exists an encrypting (N°11) but without knowing the most common method, including PKI with Public Key Certificates: 22 respondents to answer 2 of question N°15 (33%).

ITC Threats to Liberties under the Control of the Individual

Question N°3 allows us to know our respondents perception concerning the threat ITC poses to the lack of freedom. The largest majority (48%) considers that it is "certain", a median value on a scale where some consider that it is not a threat (2 individuals for answer 5) and on the contrary others esteemed that the threat is very important (4 for answer 1). However, this potential threat does not seem to weigh very heavily in terms of the answers given to question N°8 and N°9 regarding social networks : the number of Internet users using Facebook is (60 individuals for answer 1, N°8) and this several times per day (29 individuals for answer 1, N°9), or 90% and 43%. Obviously, this visibility and traceability of personal data on the Web bothers few. Nevertheless, it is impossible to ignore the social pressure: Did you see my photos on Facebook? In this context, it is interesting to cite Rousseau (1762) in the Social Contract: « In order then that the social compact may not be an empty formula, it tacitly includes the undertaking, which alone can give force to the rest, that whoever refuses to obey the general will shall be compelled to do so by the whole body. This means nothing less than that he will be forced to be free ».

The Applied Reading of Contractual Clauses on Service Provider Sites

We have determined that the respondents have a veritable blank concerning conditions stipulated by online service providers. 5 respondents to question N°16, answer 1 (8%) esteem that most providers inform Web users of inability to maintain personal data. Those Web users are however for real. A simple example from E-bay states (http://pages.ebay.com/help/policies/privacy-policy.html) : « We cannot guarantee the privacy or security of your information ».

We also learn that « We may share your personal information with Members of the eBay Inc. Corporate family – like PayPal, Skype or Shopping.com ». Finally, concerning the use of personal data for marketing purposes, the intentions are clearly expressed: « We may combine your information with information we collect from other companies and use it to improve and personalize our services, content and advertising ». Only a minority of our respondents are aware of the anonymous use of data (27 persons – answer 2), of the use of cookies (18 individuals response 3) and the sharing of consolidated data with a partner (23 Internet users – answer 4), or the following percentages successively: 40%, 27% and 34%.

Which concrete actions make it possible to limit the security risks concerning the physical and logical protection of private data? Question N°17 offers few elements for a solution. Answer 2 seems the most appropriate (25 individuals or 37% of respondents).

Table 5: Measuring Gaps in Awareness and Behaviour *(Recapitulative table of collected data)*

	awareness	**behaviour**
1. Password management	61%	13%
2. Information for online payments	74%	82%
3. Encrypting confidential data	84%	82%
4. Authentication	33%	33%
5. The threat of liberty under control	48%	90%
6. Reading contractual clauses	27%	37%

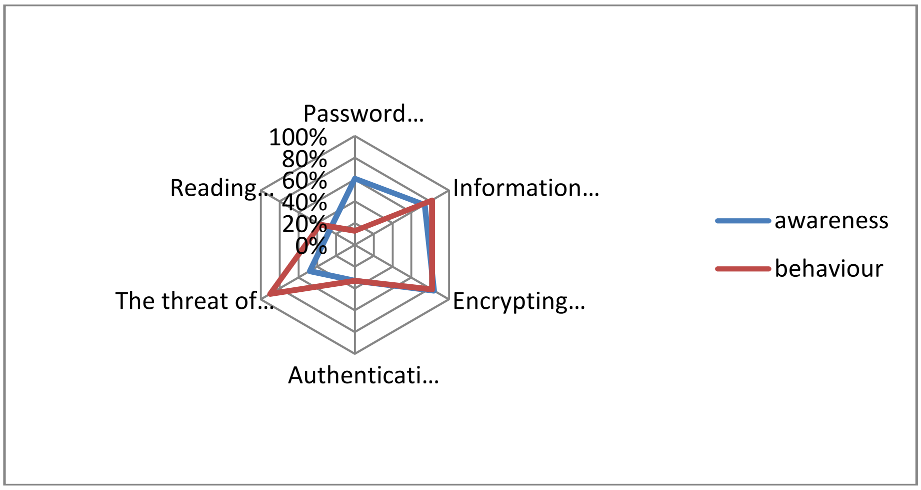

Figure 2: Analysis of Gaps between Awareness and Behaviour

Conclusion

The analysis in figure 2 shows:

- Gaps existing between awareness and behaviour are extremely weak for certain axes: encryption of confidential data, information for online payments, reading contractual clauses and authentication. There is thus an accord between awareness and behaviour.

- Important gaps exist for the axes "password management" and "threat of Liberty under control". How may these results be interpreted? Concerning the axe "password management", the awareness of the Internet users often results in the requirement of certain sites to generate a password of 6 characters; otherwise the transaction cannot be validated. This information is thus known by a majority of Internet users. However, modifying one's password or passwords requires significant work in addition for individuals who connect to numerous sites. The probability of the potential danger occurring does not incite the user to do this extra work.

- Blanks concerning the concept of authentication which is confused with the simple identification or access authorizations. Certain methods of authentication (PKI for example) are used without the sense of really being understood.

- Considerable ignorance concerning contractual clauses appearing on online service provider sites. It is understandable that many Internet users do not want to absorb entire pages relating to the security policies of online service providers.

- Finally, the overall use of the Internet is very significant but the perception of the "policing" of personal data under control does not seem to really preoccupy respondents. There would be an opportunity to better inform them of the issues.

References

Agre, P. E. & Rottenberg, M. (1998). “Technology and Privacy. The New Landscape,” *MIT Press*, Cambridge

Bloch, L & Wolfhugel, C. (2007). 'Sécurité informatique – Principes et Méthodes,' *Eyrolles*

Féral-schuhl, C. (2002). 'Cyberdroit – Le Droit à l’épreuve de l’Internet,' 3è édition *Dalloz*

Foray, B. (2007). 'La Fonction RSSI,' *Dunod*

Gearty, C. A. (2006). Can Human Rights Survive?, *The Hamlyn Lectures 2005. Cambridge University Press*, Cambridge

Gerrier, P. (2008). “Filtrage Internet : le Gouvernement met l’Accent sur la Lute

Anti-pédophilie," *ITesppresson.fr*, On line retrieve 11 june 2008, http://www.itespresso.fr/filtrage-internet-le-gouvernement-met-laccent-sur-la-lutte-anti-pedophilie-22008.html

Ghernaouti-Helie, S. (2000). "Sécurité Internet – Stratégie et Technologies," *Dunod*

Ghernaouti-Helie, S. (2009). 'La Cybercriminalité – Le Visible et l'Invisible,' *Collection le Savoir Suisse*

Hermitte, M. A. (2003). "La Traçabilité des Personnes et des Choses: Précautions, Pouvoirs et Maîtrise," *Traçabilité et responsabilité sous la dir. Philippe Pedrot, Economica*, 2003 p1-34

Kimball, R. & Ross, M. (2003). Entrepôts de Données – Guide Pratique de Modélisation Dimensionnelle, Vuibert

Larchet, S. (2010). "Google, L'arnaque Planétaire," *L'informaticien*, janvier 2010, n°76

Maiwald, E. (2004). Fundamentals of Network Security, *McGraw-Hill Technology Education*

Maret, S. (2009) 'Identité Numérique et Authentification Forte,' *Formation Continue HEC Genève*, DSSI, Module 6 3b

Martin, A. (2008). 'Facebook: on s'y Retrouve !,' *Ed. Pearson*

Mattéi, J.-F. (2003). 'Traçabilité et Responsabilité,' *Traçabilité et Responsabilité*. Pédrot P. Economica p35-44

Mitnick, K. (2003). 'L'art de la Supercherie – Les Révélations du Plus Célèbre Hacker de la Planète,' *CampusPress*

Pedrot, P. (2003). "De la Trace à la Traçabilité : des Enjeux Nouveaux pour de Nouveaux Risques," *Traçabilité et responsabilité*, Economica p.VII-X

Piatti, M. C. (2001). "Les Libertés Individuelles à l'épreuve des NTIC," *Editions PUL*

Poullet, Y. & Rouvroy, A. (2007). "Ethique et Droits de l'Homme dans la Société de l'Information," *Rapport général introductif*, Council of Europe & UNESCO, 13–14 septembre 2007, Strasbourg

Rizet, D., & Zemouri, A. (2009). "Les Photos de Treiber en Cavale," Le figaro.fr, On Line, retrieve 10/12/2009, http://www.lefigaro.fr/actualite-france/2009/10/17/01016-20091017ARTFIG00220-les-photos-de-treiber-en-cavale-.php

Rousseau, J.-J. (1762). "Le Contrat Social," Livre I,7

Shimeall, T. (2002). 'Cyberterrorism,' CERT Centers, Carnegie Mellon University

Ta, C. D. (2004). 'Démarche de Traçabilité Totale,' *Logistique & Management*, Vol.12, n°1, pp. 35-40.

Tufféry, S. (2007). Data Mining et Statistique Décisionnelle – L'intelligence des Données, *Editions Technip*