A Risk Management Process for Consumers: The Next Step in Information Security

André van Cleeff
University of Twente
Enschede, The Netherlands
a.vancleeff@utwente.nl

ABSTRACT

Simply by using information technology, consumers expose themselves to considerable security risks. Because no technical or legal solutions are readily available, and awareness programs have limited impact, the only remedy is to develop a risk management process for consumers. Consumers need to understand the IT risks they face, and decide how to deal with them in an iterative and structured manner: implement technical mitigations, alter their behavior or simply accept the risks. Such a process is feasible: enterprises already execute such processes, and time-saving tools can support the consumer in her own process. In fact, given our society's emphasis on individual responsibilities, skills and devices, a risk management process for consumers is the logical next step in improving information security.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Public Policy Issues—*Privacy*; K.6.m [**Management of Computing and Information Systems**]: Miscellaneous—*Security*

General Terms

Human factors,Legal aspects,Management,Security

Keywords

consumer, ISO27001, pCSO, personal chief security officer, privacy, risk management, security,social network

1. INTRODUCTION

As consumers' lives are revolving more and more around IT, they are facing serious security and privacy risks. But in spite of this, consumers are incapable of securing themselves. They forget to make regular backups, do not check their online banks statements and put very sensitive data on social networking sites.

At the same time, consumers are overwhelmed by well-intended advice and tools that can supposedly remedy their problems. Microsoft offers free anti-virus, the New York Times offers a three-step remedy for Facebook privacy, governments spend a great amount of money on increasing consumer 'awareness', Apple sells dedicated devices for backups, and the open source community develops software to help consumers manage their passwords.

Unfortunately, implementing, or even finding all such advice and tools would likely take more time every day than the average person is on-line. Worse, there is no proof that these 'solutions' actually work, and they will certainly not work in the near future, as consumers' use different systems and applications from day to day, and new threats emerge. As a consequence, consumers will either spend too much or too little time on security, erring on the side of too little, and their effort is ill-focused, as they do not oversee the entire range of options and do not understand the tradeoffs involved.

I argue that what consumers need most urgently is a security process: they need a structured way of dealing with the security risks they face. Executing this process is something that a government cannot do, and a government cannot make it unnecessary either by privacy legislation or consumer protection. Neither can businesses automate it completely, as the process starts with the consumer's own objectives. Ultimately responsibility for security should be placed into the hands of the consumers themselves: they must be 'in control' of their own IT devices, services and data.

First, in Section 2, we discuss two of the myriad of problems that consumers face, and why, in spite of advice and tools, they are effectively not solved. Section 3 then analyzes the problem and presents a solution, which is further elaborated in Section 4 and 5. Section 6 shows how our solution can work in practice, and Section 7 concludes the paper.

2. 'HELPING' THE CONSUMER

In this section, I will present two cases in which it is very hard (if not impossible) for consumers[1] to secure themselves adequately.

The first example concerns backups and archival and is a so-called 'critical case' that allows generalization of results [4]: In this case, it will demonstrate that even when

[1] I have chosen the word 'consumer' for two reasons: first, I wanted to set the persons (for whom the process is intended) apart from enterprises: consumers do not have the resources or the skills that an enterprise has. Second, I wanted to emphasize that the problems stem from *consuming* IT products and services. With this in mind, the reader can substitute 'consumer' with 'individual' if she wishes.

NSPW'10, September 21–23, 2010, Concord, Massachusetts, USA.
Copyright 2010 ACM 978-1-4503-0415-3/10/09 ...$10.00.

technical security mechanisms are available, and the consumer is not dependent on others, she still cannot secure her data adequately.

The second case study concerns privacy problems in social networking sites. The security problems of these sites have received a lot of attention, both from inside and outside of academia, and we will investigate the range of mechanisms that have been proposed to improve their security, and the failure thereof. As such, it functions also as a critical case, not to illustrate the problems of consumers but to show the strength of the proposed solution: I will argue in Section 6 that a risk management process for consumers will indeed work in this difficult situation, and thus it will likely work in any other situation.

2.1 Backups and archival storage

Our first example concerns the availability of data: data must be available when consumers need it. The availability requirement relates to data that is in active usage (for example recent email correspondence, the kids' homework assignments) and data that might be used later (vacation and wedding photos). With the many locations where data can be stored nowadays, both in the home and on-line, it comes as no surprise that data is frequently lost unintentionally [14]. Backups are often done ad hoc, and most of the time consumers do not know what data is archived where.

To ease archival and backups, many software applications are available, and external storage devices provide an additional level of security[2]. By connecting these devices to their computer, backups can be made automatically.

However, it is questionable whether the availability goals of the user are achieved: for example, is it actually her intention to protect the data against calamities such as fire or theft? If this is the case, then the external storage devices need to be taken out of the home periodically, which would require strict discipline and at least two storage devices to prevent loss. Thus the user likely has a less then optimal solution.

If the consumer does not want to protect her data against theft and fire, external storage devices can still protect against hard disk failure, the likelihood of which is not readily known when buying a computer. In other cases, a digital 'dustbin' helps best to retrieve documents that were accidentally deleted. Again, the user's choice of a backup solution is likely to be suboptimal.

The most reliable option for availability purposes might be remote on-line storage and backup. However, this also costs more than storage in the home, especially for large scale archival storage. Thus, for an optimal choice, the user needs to be certain that she intends to secure herself against threats such as fire and theft, and knows the cost of these solutions.

The complexity of making the right choice for backups increases when we consider that a consumer has many devices, ranging from laptops to music players, smartphones and USB sticks. Ensuring the availability of all this data requires a backup and archival plan for all of these, and the understanding of the synchronization features that are offered by software, and the risks that come along with these. Worse, much of the consumer's data is stored in the cloud. Should the user now backup data from the cloud onto her laptop? She does not know what the capabilities are of those cloud providers in terms of availability, and again is thus likely to make a suboptimal choice (or make no choice at all).

2.2 Social network sites

Our second example is about privacy on social network sites. By their very nature, sites such as Facebook[3] store personal identifiable information, often of a very private and sensitive nature. This fact alone leads to many risks, including job loss, simply being embarrassed, blackmailed [11] or having one's identity stolen [2]. Research has shown that even if users do not post explicit messages, facts such as sexual orientation can be revealed based on the connections that users have with friends [9]. Problems are aggravated, as when in the case of Facebook, users have a myriad of confusing configuration options for protecting or disclosing private information [11].

In fact, the situation is worse, as a consumer's privacy does not depend on only herself, but on many others: this is inherent to the social network infrastructure that has been built. A user can try to secure her own profile, but as long as other people upload pictures and make them available publicly, she will not achieve the goal of guarding her privacy.

In the mean time, researchers are developing technical tools to improve social network security: for example Facecloak encrypts data on Facebook to improve user privacy [13], and Clique is a social network that allows users to select audiences for their messages, rather then publish information for their entire network[4]. Another approach is taken by Diaspora, where users store their information on their own servers instead of depending on commercial sites that they cannot control[5]. However, although technically sound, such tools need to be in widespread usage to be effective: anyone using them will likely spend much time on migration and configuration, as well as convincing their friends to use it too.

Another approach to improve social network security is legal action: the European Union is considering new legislation to protect the privacy of its citizens[6], and nonprofit organizations such as the Electronic Frontier Foundation (EFF) have pressurized enterprises with the same goal. Whether these initiatives are effective remains in doubt, as each technology brings on new privacy problems, and legislation lags behind these technologies.

Governments also attempt to educate citizens with awareness initiatives, which so far have had a very limited effect[7]. Users are given extensive advisories for altering their behavior and changing their privacy settings [15]. Unfortunately, Facebook continues to introduce new features and new types of privacy controls, so the consumer has to keep reading the news to find what new rules and settings she should apply. For example, in April 2010 a service called 'instant

[2] For example Microsoft's Windows Live OneCare Backup and Restore, and Apple's Time Machine and Time Capsule

[3] Because Facebook is the largest social network, and the most widely researched, all examples in this paper concern Facebook. I do not imply that Facebook is less or more secure than any other social network site.

[4] http://clique.primelife.eu/

[5] http://www.joindiaspora.com/index.html

[6] http://www.businessweek.com/globalbiz/content/jan2010/gb20100129_437053.htm

[7] http://www.cytrap.eu/files/info/2007/pdf/2007-10-18-CertGovNL-Presentation-fin-online.pdf

personalization' was launched, which allows users to share information with other websites [16] by default. Thus the user is likely to end up exposing herself more than she intends.

Given the security problems of social networking sites, the best advice might be to simply stop using Facebook. Whether this is in the interest of the consumer depends on the tradeoffs she makes between the social functions that these sites offer and the consequential loss of privacy. Unfortunately, the consumer does not know how to make this tradeoff, as it is beyond the scope of any advice or tool created.

2.3 Evaluation

Our two samples of IT usage show that even in very common cases, which millions of consumers face, consumers are unable to secure themselves efficiently. In the case of backups, technical solutions exist, but consumers do not have the means to decide which solution fits their goals best, and how to adapt to changes in their life, such as using new applications or IT products.

In the case of social network sites, we see that even the mix of technical and legal measures and awareness programs does not solve the consumer's privacy problems. Thus, the consumer's security situation is suboptimal, not only for these cases, but likely concerning her entire usage of IT.

3. PROBLEM ANALYSIS AND SOLUTION

From the case studies in the previous section, we learn that consumer security is neither effective nor efficient. We will now summarize the main problems and solutions in Section 3.1 and show how we can learn from enterprises in Section 3.2.

3.1 Consumers need a security process

First, consumers need to state their *goals* explicitly, what they actually wish to achieve. As consumers do not start out by setting specific security goals, they cannot make informed decisions and live up to them, so that they have a decent strategy for their backups or for guarding their privacy.

Second, if the consumer decides whether to use an application, the consequences should be clear: what are the *tradeoffs* involved, for example in terms of money and privacy? This involves also *risk management*, assessing how likely certain threats are against assets, and what can be done to mitigate them.

Third, securing IT is essentially a *cyclic* process. Checklists have to be executed periodically because the consumer's own goals change, new technology is introduced, and security processes degrade over time. Each change requires a re-evaluation of the situation. Combined, the central thesis of this paper is that:

Out of all possible technical, legal and other measures that can improve consumer security, a risk management process will have the most impact.

3.2 The enterprise security process

Having stated the requirements for a consumer security in the previous section, the question can be posed how likely it is that these requirements can be realized. In this context, we examine the enterprise security process, which demonstrates that in another context, such requirements are already fulfilled: there are methods to implement a goal-driven, cyclic security process to make risk assessments.

Concerning the goals, the governance structure of enterprises is laid out in frameworks such as COSO[8]. Business goals are determined by the CEO, and the CIO (Chief Information Officer) and CSO (Chief Security Officer)[9] translate business requirements into IT and security goals, and finally into policies, choosing the most effective security mechanisms, in the context of a security program.

ISO 27001 specifies how an Information Security Management System (ISMS) can be implemented [8]. This 'system' is actually a cyclic security process, consisting of four phases:

1. Plan (establish the process)
2. Do (implement and operate the process)
3. Check (monitor and review the process)
4. Act (maintain and improve the process)

Risk assessment is part of the establishment and management of the ISMS process. First the enterprise sets criteria for how much risk the company in general is willing to take, the 'risk appetite'. Next, risk identification is performed: a risk assessment team considers the threats to company assets. The risks are analyzed and options for risk treatment considered. In general, four options exist to treat risks:

1. Accept (do nothing)
2. Transfer (for example buy insurance)
3. Mitigate (put security controls in place)
4. Avoid (discontinue the activity)

Note that there is no normative judgment involved: taking more risk is not necessarily bad, as spending too many resources on security will not benefit customers, employees or shareholders.

In essence, such a process should be available for consumers as well. Therefore, in order to solve the consumer security problem, consumers will have to adopt a framework similar to that of ISO 27001, but sufficiently simple so that it can be executed by a non-skilled person, in limited time.

4. COUNTERARGUMENTS

We will now discuss several counterarguments for our thesis that consumers will benefit from executing a security process, and are capable of executing it.

4.1 Consumers do not know what they want

In an enterprise, success is definable by monetary loss or profit, and a business can relate its security mechanisms to these goals, to determine how much effort should be spent on security. However consumers, especially in their private life, do not have clearly defined goals, and hence it is not clear what mechanisms they should put in place and at what cost [18]. Furthermore, there is doubt about whether consumers actually have stable privacy preferences [1].

[8] `http://www.coso.org/`

[9] The CISO title (Chief Information Security Officer) is also widely used, but I prefer the term CSO here, because the security process proposed here should ultimately also consider home automation systems, which are more in the domain of physical security than of pure information security.

Response.

In the context of social networks, evidence exists that user's have a specific set of goals, and that they are capable of performing a tradeoff between the goals of privacy and of meeting new friends [10]. Therefore, it can be argued that a goal-driven risk management process for consumers simply supports their existing practice. Even if consumers cannot state their exact goals, they likely know what they do *not* want: consumers can be shown a list of threats, and they choose whether they wish to avoid them: whether they want to run the risk of losing their job because of Facebook, or accept the loss of data in case of a fire. Tools and techniques to elicit security and privacy goals are available [12]. Naturally, changes in consumer's goals are expected, and the cyclic nature of the process allows (or even invites) consumers to alter their policies because of actual changes or simply because they view privacy differently.

4.2 Consumers do not think, they do

In an enterprise, security is institutionalized: employees perform different functions, check the performance of others', and guard their part of the process. A CSO has a real responsibility; she can be fired if too many incidents occur. For a consumer, security will always be a secondary objective, and she cannot be fired or replaced. Furthermore, this institutionalization slows down changes and this latency can be considered a good thing: an organization with good security policies cannot lose them overnight. By contrast, consumers act very fast, they can decide in minutes to buy a new computer and start using it immediately, without any formal process taking place. Creating a new Facebook account takes no more than a minute.

Response.

Indeed, consumers act faster, but many processes can be automated, as we will see in Section 5. Furthermore, the cyclic nature of the process (plan-do-check-act) makes it possible to detect violations of policies and correct them afterwards, limiting the impact.

4.3 Consumers do not want to spend time on security

Ultimately, security and privacy is of little value to consumers, and this is why many consumers refuse to put in much effort. For example, according to one calculation, given the likelihood of phishing (resulting in fraud) efforts to prevent it should not take more than a second a day to be economically feasible [7].

Response.

The security process must become an integrated part of what people do. Taking care of one's security can become something similar to mowing one's lawn, or cleaning up one's home: no one questions the economic value of these activities, because social norms require it. Currently the lack of security, and the social consequences thereof, is not clearly visible, but a risk management tool will address precisely this problem, by giving consumers the option to share their risk assessment results, and explain how they protect their own data and that of others.

Arguably, consumers can spend relatively less time on security than enterprises: they do not own large IT infrastructures comprising hundreds of servers, where the likelihood must be estimated that attackers will move from node to node in a long multi-step attack [5]. For consumers, a cloud computing service can simply be considered as a black box. Also, proper tools (which are lacking to prevent the previously mentioned phishing attacks) can reduce the time that users must spend on security.

4.4 Consumers are stupid

Consumers do not have any expertise in risk assessments, and especially people with little formal education will not be able to execute a whole risk assessment process.

Response.

Many parts of the process can be automated, and there is no requirement for understanding everything into detail. Some things are naturally complicated, but consumers are free to spend time as they see fit. If someone chooses to spend less time on learning her security process, she will likely have less security, but maybe this is the most ideal situation, the optimal tradeoff between effort and result. In an enterprise context of managing IT, maturity models are used (such as for CObIT[10]) for this purpose. A-priori, there is nothing wrong with being at a low maturity level - but consumers should nevertheless make a conscious decision about their security - and do this repeatedly, starting with their security goals.

4.5 A consumer security process will stifle innovation

If users have to consider security before signing up to a new service, they will never use it, and there will be no new Android, Twitter or iPhone, and consumers will be ultimately worse off in terms of security.

Response.

If the new service offers security guarantees from the start, it will even improve adoption. Rather than stifling innovation, a consumer security process will spawn many new areas of research, and provide many opportunities to innovate. In fact, users will be able to use more products and services securely, not being held back by worries about their security.

5. TOWARDS A PERSONAL CHIEF SECURITY OFFICER

After having discussed and rejected several counterarguments in Section 4 we now focus on envisioning an actual solution. We call the tool the 'personal Chief Security Officer' (pCSO). Figure 1 shows the tool in its context, and its features are explained next.

5.1 Architecture

The architecture of the pCSO consists of four main components:

- a personal user interface and database with which the consumer interacts

- a shared risk repository that stores threats, vulnerabilities and other risk-related information, shared between consumers

[10] `http://www.isaca.org/cobit/`

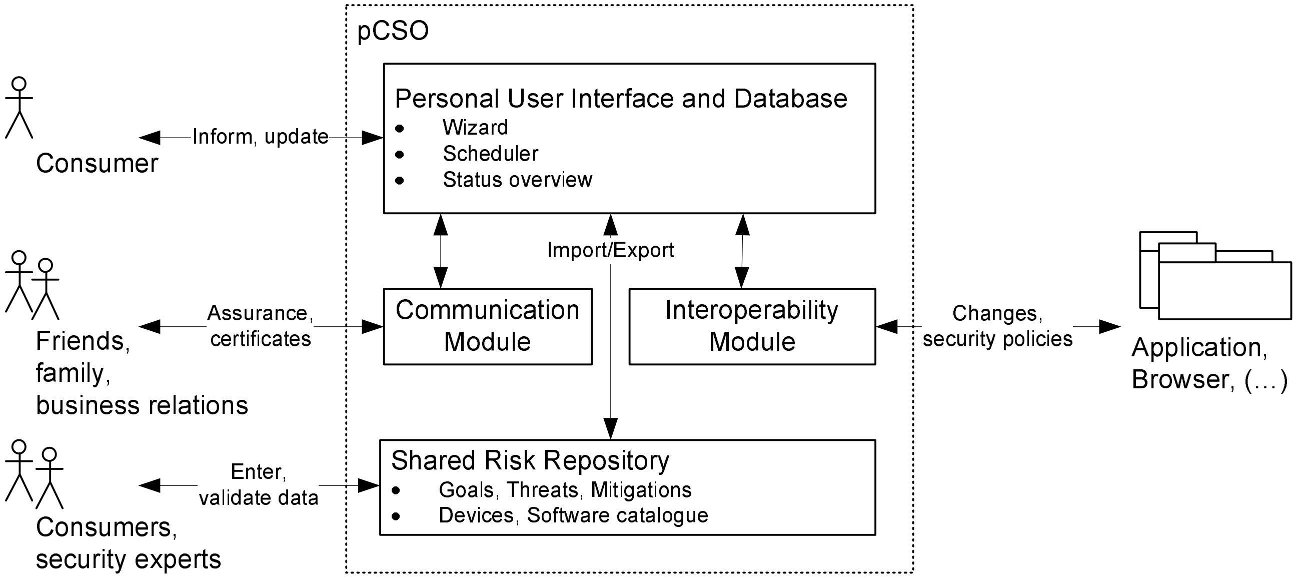
pCSO
Personal User Interface and Database
Wizard
Scheduler
Status overview
Consumer
Inform, update
Import/Export
Friends, family, business relations
Assurance, certificates
Communication Module
Interoperability Module
Changes, security policies
Application, Browser, (...)
Consumers, security experts
Enter, validate data
Shared Risk Repository
Goals, Threats, Mitigations
Devices, Software catalogue

Figure 1: The personal Chief Security Officer in context

- an interoperability module for reading configuration and status information from devices and applications
- a risk communication module for communicating risks statements between consumers

Next, we will discuss each of this in further detail.

5.2 Personal user interface and database

The pCSO offers a *dashboard*, providing a status overview. Opposite of other privacy dashboards such as offered by Google[11], the pCSO dashboard aggregates information from all applications and systems the consumer is using, not just from one vendor. The dashboard displays the entire IT infrastructure that the consumer owns or uses, and the data stored on it: devices such as notebooks and smartphones, applications in use, and data such as email, music and chat logs. Next, the dashboard gives insight into the risks, showing how much risks the user is exposed to. It shows information about all security properties: confidentiality, integrity and availability. Opposite of many awareness campaigns and advisories, which give consumers the impression that they can secure themselves perfectly if they implement a small set of measures, the pCSO clearly presents the residual risks that consumers are exposed to. These risks exist in various forms:

- Caused by not implementing available mitigations. For example, a user can choose not to use strong passwords.
- Caused by technological limitations. For example, while browsing normally, data is transferred in plain text over the Internet, leading to privacy problems.
- Caused by goal conflicts. For example, if the business goal of a service provider is to gather data about users, and the consumer's goal includes privacy, there is a structural threat, caused by the two conflicting goals, regardless of the legal or technical context.
- Caused by other people's risk exposure. For example, a consumer's chat history is also stored on friends' computers.

All information from the consumer's own risk management process is stored in the personal database. It contains a complete overview of her goals, the IT systems that she owns and the tasks that she has performed and has to do (such as risk assessments) in order to manage her risks.

A *wizard* helps consumers to configure their security process easily. It takes consumers through a series of steps, defining the devices and data they have, their security goals and informs them about the threats they have and how to mitigate them. To prevent the user from being cluttered with information, several filters are applied in this process:

- user's expertise (exclude mitigations that are complex)
- user's available time (exclude mitigations that take more then 15 minutes)
- user's own infrastructure (exclude threats related to social networking sites, if the user does not use them)
- user's goals (exclude financial threats if the user is not concerned about her financial status)

Finally, a *scheduler* will contact the user at regular intervals, to assess whether any changes have taken place, which need to be taken into account. If necessary, this leads to a new task for the user.

5.3 Shared risk repository

Although the pCSO is intended to be used as an individual tool, data should be shared, to execute the security process effectively. A central repository contains frequently used data, which consumers do not have to invent and enter themselves:

[11] http://googleblog.blogspot.com/2009/11/transparency-choice-and-control-now.html

- security goals, such as keeping one's job
- devices, similar to an infrastructure library, for example listing all the iPhone models
- software catalogue, containing widely used software, with features and configurations, for example all Windows versions
- attacks and mitigations, for example risks relating to identity theft

Such databases already exist for commercial purposes, for example the CRAMM methodology (in use by NATO), has an extensive database of security controls[12]. The pCSO shared risk repository can be maintained in a collaborative effort by consumers, enterprises and security researchers.[13]

5.4 Interoperability module

The interoperability module links the pCSO to other tools and applications. The goal is to make the risk management process work faster and easier. For example, to populate the list of applications that the consumer uses, the module scans the browser history. When the user then logs on to a social network service, this application is added to the personal database, and risk-related data on this application is retrieved from the shared database. Next, the pCSO alerts the consumer of actions that she can or should take to comply with her own policies. By contrast, the consumer's policies might be such that the usage of the application is simply in violation of her own security policies: she is given the choice between either changing her policies or abandoning the intent of using the application.[14]

Possibly, the pCSO can use the previously developed Platform for Privacy Preferences (P3P) by the W3C[15], which allows browsers to process website's privacy policies automatically.

5.5 Risk communication module

The risk communication module helps to share risk assessment results between users: data gathered by the pCSO can be passed on to others, providing evidence that a person has spent effort on maintaining her security posture, possibly even demonstrating compliance with certain regulations, which is needed in a business environment (for example when working as a freelancer). The module can also send requests for such results and indicate what types of measures the recipient is expected take.

6. REALLY HELPING THE CONSUMER

To illustrate how the pCSO will work in practice, we will return to the cases of Section 2, and show how a pCSO gives consumers more control over their security, and likely improve her security posture. First Alice uses the pCSO for ensuring data availability, second Bob manages his privacy with the pCSO.

6.1 Backups and archival storage

If Alice is using the pCSO, her laptop is already registered in her personal database, and the pCSO automatically scanned the laptop for her files such as emails, photos, movies. She then determines how this data support her goals: communicating with friends, maintaining a personal archive, gaining an income through her work as an independent consultant. Next, the pCSO informs her of the threats she is exposed to, including data loss because of theft, fire and mechanical failure. (The pCSO informs her of the likelihood of a disk crash, using the laptop's manufacturer and serial number.) Taking into account how the data helps to realize her goals, she determines the risks she is willing to take. She accepts the loss of data during travel, but wants to have a backup in case of fire. The pCSO then presents her with a list of mitigations, including online backups and external storage devices. Taking the cost of each of these into account, she decides to settle for external storage devices. The pCSO then provides her with a standard operating procedure to effectively manage the risks: she will store one device in her home, and one in her office. Every two weeks, the pCSO gives a reminder that the devices need to be swapped, after which she initiates the backups. After two months, she buys a new smartphone, which she registers in the pCSO. The dashboard now shows that she has not defined the data availability goals for this phone and the data residing on it: she registers that the smartphone synchronizes with the laptop, and that the laptop is the master copy, from which she will be making backups. Working with the pCSO in this way, Alice feels confident that here data is secured and will be secured in the future.

6.2 Social network sites

Bob (a high ranking government official) starts by selecting his goals from the list provided by the pCSO. The wizard helps him to decide the importance of these goals, based on his personal situation, as for example many goals are dependent on age [10]. Concerning the social network site, Bob indicates that it contributes to the goals of presenting a positive and public profile, and maintaining contact with friends. The pCSO indicates that these goals conflict, and informs Bob of the threat of privacy loss: this cannot only have an impact in the near future but also for his future career.

Based on this consideration, Bob considers the trade-offs between these goals, and the options for mitigating this risks. He decides to limit privacy risks by keeping his profile mostly empty. On the social network site, he will keep a minimum profile and not upload any personal pictures. Every month, the pCSO reminds him to check whether he has been 'tagged' in photos, after which he can take action (have the pictures removed if inappropriate). After a while, Alice wishes to become Bob's friend on the site. Before accepting her, he wishes to know her security posture: as she is using the pCSO with certain privacy policies, he requests her status report, so he can assert that she will take his privacy seriously. She sends the report by the pCSO using the risk communication module and he accepts her request. A week later, the networking site that Bob uses changes its policies. Many pCSO users notice this change, and an advisory is created in the shared risk repository. As Bob is a user of the site, a message is displayed on his computer, which instructs him how to deal with the change, keeping in line with his

[12] http://www.cramm.com/capabilities/controls.htm

[13] The problems of maintaining an accurate and reliable database and their solutions are out of the paper's scope

[14] Communicating impending security risks effectively to end-users has been investigated earlier by Sunshine et al [17].

[15] `www.w3.org/standards/techs/p3p\#w3c_all`

own policies. Thus, Bob is assured that he has done the right steps to prevent damage to his career.

7. CONCLUSION

If someone would audit consumers, they would not be 'in control' of their assets, with unknown, potentially dire consequences for their own security, and that of their friends, family and business relations. In this paper, I have argued that the one thing that can improve information security in the short term is to develop a security process for consumers, such that they can regain control. Technical solutions to security such as privacy-enhancing techniques are not readily in use, and little can be expected from changes in laws and regulations and changing social norms and practices. The only immediate thing that can be done, is to give consumers the tools for doing risk assessments, accepting the existing infrastructure (technical, legal, social) as a given. All the resources spent on raising 'awareness' are more effectively spent on creating this process, because arguably, the process is the necessary precondition for sufficient awareness, and *not* the consequence.

Realizing a consumer security process will not be an easy task, but it is feasible, and it will be worth the effort. As the investigation of enterprise security has shown, many parts of the solution already exist, and can be adapted for consumers.

There is no one better suitable for securing her assets than the consumer herself: she has the best knowledge about her own situation, and the best motivation to do it. With the trend of consumers working on their own devices (opposite of having shared computers), a consumer security process is the logical next thing to be developed: Everyone has to manage the security of her own 'lifestream', the time-ordered stream of documents that is created in the process of her life [6].[16]

Furthermore, with the ever increasing workforce of independent contractors and freelancers, it does not suffice - even for enterprises - to focus on enterprise security. If the freelancer's Blackberry is not secured, it is not only her own shop that is at risk, but also the enterprise's that hires her.

In the near future IT will not only affect our digital (or social) security, but also our physical environment: the smart homes of the future will be equipped with medical devices, digital door locks and smart energy meters. Without a process in place to manage this abundance of IT, the consumer will not have control anymore.

Developing the tools to support this process will not only have a direct impact on the security of individuals and enterprises, but more importantly, it will be a catalyst for the development of new devices and software: as it makes people conscious of the shortcomings of existing solutions. Thus, although our future will be filled with new devices and software, we will be better equipped for dealing with them.

Acknowledgment

This research is supported by the research program Sentinels (www.sentinels.nl). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs under project number TIT.7628.

8. REFERENCES

[1] A. Acquisti. Nudging Privacy: The Behavioral Economics of Personal Information. *IEEE Security and Privacy*, 7(6):82–85, 2009.

[2] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web*, pages 551–560. ACM New York, NY, USA, 2009.

[3] EU Directive. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. *Official Journal of the EC*, 23, 1995.

[4] B. Flyvbjerg. Five misunderstandings about case-study research. *Qualitative inquiry*, 12(2):219, 2006.

[5] V. Franqueira, R. Lopes, and P. van Eck. Multi-step attack modelling and simulation (MsAMS) framework based on mobile ambients. In *Proceedings of the 2009 ACM symposium on Applied Computing*, pages 66–73. ACM, 2009.

[6] E. Freeman and D. Gelernter. Lifestreams: a storage model for personal data. *ACM SIGMOD Record*, 25(1):80–86, 1996.

[7] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *NSPW '09: Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144, New York, NY, USA, 2009. ACM.

[8] International Organization for Standardization (ISO/IEC). ISO/IEC 27001:2005 Information technology – Security techniques – Code of Practice for Information Security Management, 2005.

[9] C. Jernigan and B. Mistree. Gaydar: Facebook friendships expose sexual orientation. *First Monday*, 14(10-5), 2009.

[10] A. Joinson. Looking at, looking up or keeping up with people?: motives and use of Facebook. In *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, pages 1027–1036. ACM, 2008.

[11] H. Lipford, A. Besmer, and J. Watson. Understanding privacy settings in Facebook with an audience view. *Usability, Psychology, and Security*, 2008.

[12] L. Liu, E. Yu, and J. Mylopoulos. Security and privacy requirements analysis within a social setting. *IEEE International Conference on Requirements Engineering*, 0:151, 2003.

[13] W. Luo, Q. Xie, and U. Hengartner. FaceCloak: An Architecture for User Privacy on Social Networking Sites. In *International Conference on Computational Science and Engineering*, volume 3, 2009.

[14] C. Marshall. Rethinking personal digital archiving, part 1. *D-Lib Magazine*, 14(3):2, 2008.

[16] Note that this viewpoint is somewhat in opposition with for example the European Union's Directive 95/46/EC on data protection, which only offers guidelines for enterprises [3], and explicitly exempts natural person from taking security precautions, when data is gathered in the course of a purely personal or household activity.

[15] New York Times. Three settings every Facebook user should check, January 20 2010. www.nytimes.com/external/readwriteweb/2010/01/20/20readwriteweb-the-3-facebook-settings-every-user-should-c-29287.html, Retrieved 2010-04-24.

[16] R. Richmond. How to Opt-Out of Facebook's Instant Personalization. New York Times, April 24 2010. gadgetwise.blogs.nytimes.com/2010/04/23/how-to-opt-out-of-facebooks-instant-personalization/, Retrieved 2010-04-24.

[17] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. Cranor. Crying wolf: An empirical study of SSL warning effectiveness. In *Proceedings of the 18th Usenix Security Symposium*, 2009.

[18] A. van Cleeff. Future consumer mobile phone security: A case study using the data-centric security model. *Information Security Technical Report*, 13(3):112–117, 2008.