A Risk Management Process for Consumers: The Next Step in Information Security (Position Paper)

André van Cleeff
University of Twente
P.O. Box 217, 7500 AE 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, the only remedy is to develop a risk management process for consumers, similar to the process executed by enterprises. Consumers need to consider the risks in a structured way, and take action, not once, but iteratively. 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.

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 the 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 discuss the problems that consumers[1] are facing, to show why, in very simple cases, it is very difficult for consumers to get their security right. The first case study concerns backups and archival, the second social networking sites. For each case, I briefly illustrate the security problems that arise, and discuss some of the shortcomings of available devices and the advice given. I do not intend to be exhaustive, similar problems that consumers need to deal with are abundant (consider securing USB sticks and smartphones or managing passwords).

2.1 Backups and archival storage

Our first example concerns the availability of data: most consumers want their data to be available when they 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

[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.

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 [11]. 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 safety[2]. By connecting these devices to their computer, backups can be made automatically.

However, it is questionable whether the 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 suboptimal 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. 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 contain personal identifiable information, often of a very private nature. This leads to many risks, including job loss, simply being embarrassed, blackmailed [8] or having one's identity stolen [2]. Privacy advocating organizations such as the Electronic Frontier Foundation (EFF) have come in very hard on these issues, to ensure that enterprises protect the privacy of their users. The media follow these battles with interest and regularly publish information intended to remedy the situation. For example, in January 2010, the New York Times published an advisory concerning Facebook privacy settings [12]. Facebook also 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. The most recent example in April 2010 concerns a new service called 'instant personalization', which allows users to share information with other websites [13] by default. Thus she is likely to end up exposing herself more than she intends.

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 tools to shield data on social network sites from others: for example Facecloak encrypts data on Facebook to improve user privacy [10]. However, although technically sound, such tools need to be in widespread usage to be effective: anyone using them will spend an unreasonable amount of time on implementing it and making sure their friends use it too. If the consumer is seriously concerned about privacy, the best advice might be to simply stop using Facebook. Whether this is a good advice depends on the tradeoffs the user makes between the social functions that Facebook offers and the consequential loss of privacy. However, 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 will be unable to secure themselves efficiently. In the case of backups, a vendor tries to sell a product that only partially solves the probable goal that the user has. In the case of social network sites, we see that solutions are ad hoc; making it likely that in the future the consumer will have lower protection, unless magically, she stumbles upon a new piece of advice that guides her in the right direction. 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 very effectively nor efficient. We will now summarize the main problems 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?

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

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

- new technology is introduced
- security processes degrade over time
- the consumer's own goals change

Each change requires a re-evaluation of the situation. Combined, the central thesis of this paper is that
consumers need a goal-driven, cyclic security process to make risk assessments. Until this process is in place, all other attempts at securing consumers will fall far short.

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[3]. Business goals are determined by the CEO, and the CIO (Chief Information Officer) and CSO (Chief Security Officer) 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 [7]. 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 less risk is not necessarily bad, as spending too many resources on security will neither benefit customers nor 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 [14]. Furthermore, there is doubt about whether consumers actually have stable privacy preferences [1].

Response. Consumers also know what they do *not* want: consumers can be shown a list of risks, 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 [9]. Furthermore, changes are expected, 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. Oppositely, consumers act very fast, they can decide in 20 minutes to buy a new computer and start using it immediately, without any formal process taking place. Creating a new Facebook account takes even less time.

Response. Indeed, consumers act faster and have less interest, 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.

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

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 more 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 [6] to be economically feasible.

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, they have to be done. Currently the lack of security is not visible, but once others take notice, consumers will make sure that it is in order. It can also be argued that consumers will spend certainly less time 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 [4]. For consumers, a cloud computing service can simply be considered as a black box. However, it is unquestionably true that there is a bootstrapping problem.

4.4 Consumers are stupid

Consumers do not have any expertise in risk assessments, and especially people with little 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[4]) 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 more securely, not being held back by worries about their security.

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

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), and its features are explained next. Figure 1 shows the tool in its context.

5.1 Core functionality

The core of the pCSO consists of three main components, with which the consumer interacts.

First, 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.

Second, 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 task for the user, for which the wizard is invoked.

Third, the pCSO offers a *dashboard*, providing a status overview of the entire IT infrastructure that someone has, the risk exposures, deficiencies and points of attention. Opposite of other privacy dashboards such as offered by Google[5], the pCSO dashboard aggregates information from all applications and systems the consumer is using, not just from one vendor. Here, the user can see which applications she is using, what devices she has, and what actions need to be taken. Part of the status overview is an indication of how well the user is managing her security. The dashboard shows information about all security properties: confidentiality, integrity and availability.

5.2 Shared data

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

- 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[6]. The pCSO library can be maintained in a collaborative effort by consumers, enterprises and security researchers.

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

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

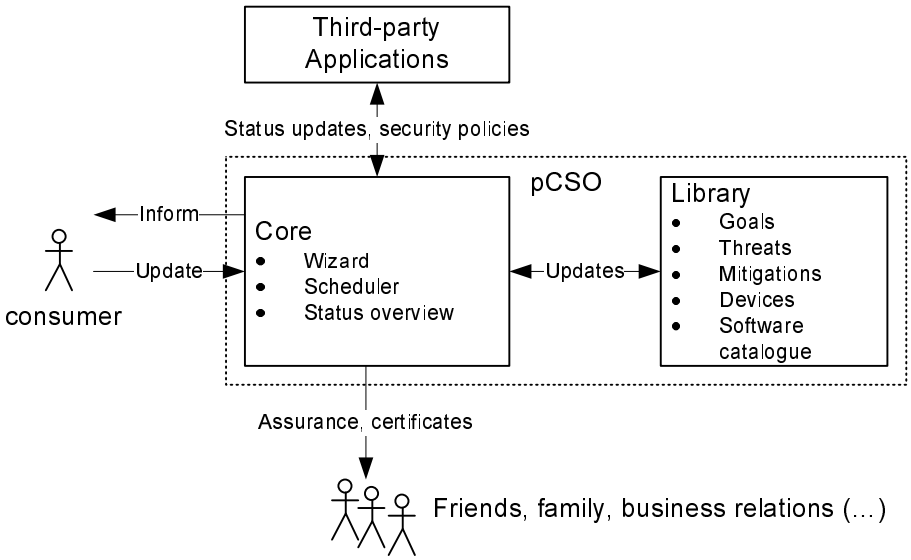

Figure 1: The personal Chief Security Officer in context

It should also be possible to share risk assessment results between users: data gathered by the pCSO can be passed on to others, proving 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).

5.3 Interoperability with applications

Interoperability with other applications can make the process work faster and easier. For example logging into a social network service can automatically trigger an event that this particular application is used, and alert the consumer of actions that she needs to take. Oppositely, 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. This approach could make use of the previously developed Platform for Privacy Preferences (P3P) by the W3C[7], which allows browsers to process website's privacy policies automatically.

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 would give consumers more control over her 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

Alice enlists her laptop in the pCSO through the wizard. She clicks the types of data that she has (personal and work emails, photos, movies), and 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 informs her of the likelihood of a disk crash, using the laptop's manufacturer and serial number.) Next, she buys two external storage devices; one is located 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 policies 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 starts by enlisting his goals. Since Bob has a high profile and very visible job position, the pCSO warns him extensively of the risks that he runs by using the social network site - not only now but also in the decades to come. Based on this consideration, Bob decides to keep a minimum profile, not uploading any 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). After a while, Alice wishes to become Bob's friend on the site. Before accepting her, he investigates her security posture: as she is using the pCSO with certain privacy policies, he asks for her status report, so that he can assert that she will take his privacy seriously. She sends the report by the pCSO and he accepts her request. A week later, the networking site changes its policies. Many pCSO users notice this change, and an advisory is created in the shared library. As Bob is a user of the site, it pops up on his computer, and instructs him how to deal with the change, keeping in line with his 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, but likely dire con-

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

sequences 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; the only immediate thing that can be done, is to give consumers the tools for doing risk assessments, accepting the existing infrastructure 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. 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 [5].[8]

Furthermore, with the every 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 individual's and enterprise's security, 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 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]Note that this viewpoint is somewhat in opposition with for example the European Unions 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.

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] 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.

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

[6] 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.

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

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

[9] 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.

[10] 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.

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

[12] 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-shoul` `html`, Retrieved 2010-04-24.

[13] 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.

[14] 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.