A Case for Societal Digital Security Culture

Lotfi Othmane, Harold Weffers, Rohit Ranchal, Pelin Angin, Bharat Bhargava, Mohd Mohamad

A Case for Societal Digital Security Culture

Lotfi ben Othmane[1], Harold Weffers[1] Rohit Ranchal[2], Pelin Angin[2], Bharat Bhargava[2], and Mohd Murtadha Mohamad[3]

[1] Laboratory for Quality Software, Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands
{l.ben.othmane,h.t.g.weffers}@tue.nl
[2] CERIAS and Computer Sciences, Purdue University, USA
{rranchal,pangin,bb}@purdue.edu
[3] Faculty of Computing, Universiti Teknologi Malaysia, Malaysia
{murtadha}@utm.my

Abstract. Information and communication technology systems, such as remote health care monitoring and smart mobility applications, have become indispensable parts of our lives. Security vulnerabilities in these systems could cause financial losses, privacy/safety compromises, and operational interruptions. This paper demonstrates through examples, that technical security solutions for these information systems, alone, are not sufficient to protect individuals and their assets from attacks. It proposes to complement (usable) technical solutions with Societal Digital Security Culture (SDSC): collective knowledge, common practices, and intuitive common behavior about digital security that the members of a society share. The paper also suggests a set of approaches for improving SDSC in a society and demonstrates using a case study how the suggested approaches could be integrated to compose a plan for improving SDSC.

Keywords: Information Security, Security Culture, Security Usability

1 Introduction

We commonly use pervasive computing systems, such as remote vehicle control systems [1], remote healthcare monitoring systems, and home automation systems to improve our life quality; public information systems [2], such as online banking for personal business; and Internet telephony applications, such as Skype for personal communication. However, these systems have security threats–circumstances and events with the potential to harm an Information System (IS) through unauthorized access, destruction, disclosure, modification of data, and Denial of Service (DoS) [3].

Attackers exploit technical vulnerabilities and security policy violations to trigger security threats and compromise the system's assets. Technical vulnerabilities are weaknesses and flaws in a system's design, implementation, or operation and management [4]. For example, sending data through networks without assuring confidentiality and integrity [4] is a weakness of the system that manages them. Policy violations are faults in applying and enforcing security policies that provide attackers with confidential information or technical weaknesses

Table 1. Impacts of security threats to systems.

Impact	Example
Safety compromise	Attacker controlling the brakes of a vehicle [6] through remote access to the in-vehicle network of the vehicle using a mobile phone.
Financial loss	Attacker installing a key logger on the mobile device of a user to capture credentials for performing financial operations on his behalf [7].
Privacy violation	Use of information on an Online Social Network (OSN) for purposes they were not intended, as in the case of a teacher in training being denied her teaching degree due to her photos posted on an OSN [8].
Operational interruption	Attacker continuously sending messages to a vehicle to prevent it from sending e-call messages to a service center in case of an accident [9].

which allow them to compromise assets of the system. For example, an attacker could use social engineering [5] to get the secret password of an individual for online banking (e.g., when he/she gets drunk), which enables him/her to withdraw money from the victim's bank account. Table 1 provides an overview of the impacts of major security threats to information systems.

Figure 1 shows that the security threats for information systems we use fall into several categories: physical security violations, technical attacks, security policy violations, and errors caused by limited human knowledge. Technical security measures attempt to address these threats, but fall short in providing comprehensive security solutions in most cases.

This paper investigates two main questions: What are the limitations of technical security solutions used in pervasive systems, social networks, and public information systems? And, how can technical security solutions be supported to reduce the risks of security threats to these systems? We answer the first question through analyzing the efficacy of technical security mechanisms for two case studies: connected vehicle and online banking. The analysis shows that technical security solutions, alone, cannot protect individuals and their assets from attacks. Therefore, we propose to extend the technical solutions with Societal Digital Security Culture (SDSC), which answers the second question.

Digital Security Culture (DSC) in organizations is well investigated, e.g. [19], [20], and [21]. However, to the best of our knowledge, Colella and Colombini [22] are the only authors who–briefly–discussed security awareness to address threats related to pervasive computing. There is currently no work on SDSC. The main contributions of this paper are to: (1) demonstrate that technical security mechanisms, alone, cannot sufficiently protect individuals and their assets from attacks on systems they use, (2) propose to extend technical security mechanisms through SDSC, and (3) suggest approaches for improving SDSC.

The rest of the paper is organized as follows: Section 2 describes the limitations of efficacy of technical security solutions. Section 3 provides an overview of "usable security" and its limitations. Section 4 defines and describes SDSC. Section 5 suggests some approaches for improving SDSC, Section 6 presents an

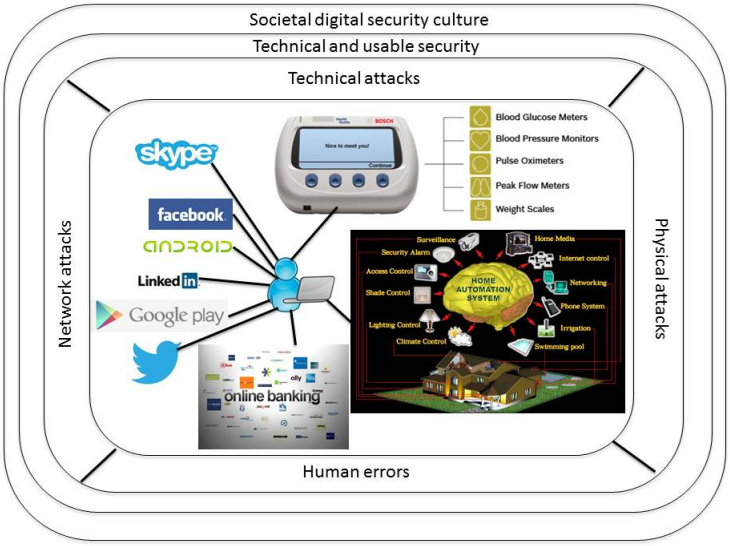

Fig. 1. Security environment for everyday information systems. (Image references clockwise from top right corner: [10], [11], [12], [13], [14], [15], [16], [17], [18].)

example for reducing the risk of security threats through improving SDSC, and Section 7 concludes the paper.

2 Limitations of Efficacy of Technical Security Solutions

2.1 Overview of the limitations of technical solutions

Companies which develop systems and applications for public use implement technical security solutions, which cannot alone prevent and protect the user of the systems or applications from attacks (even if they were certified to assure the security of the user). The main limitations of the technical solutions are:

L1. *Policy violation.* Technical security solutions often rely on the user to comply with some security policies, e.g., not disclose a password. However, a user may violate the policy, e.g., provide his/her password to other individuals.
L2. *Weak mechanisms.* Companies often implement ineffective security solutions for protecting users' assets, so they preserve low product cost. For example, pacemakers and implantable cardiac defibrillators have weak security mechanisms although they are widely used [23].
L3. *New attack scenarios.* Companies implement security mechanisms for known attacks. However, attackers attack where they are least expected; they discover new vulnerabilities and exploit them.

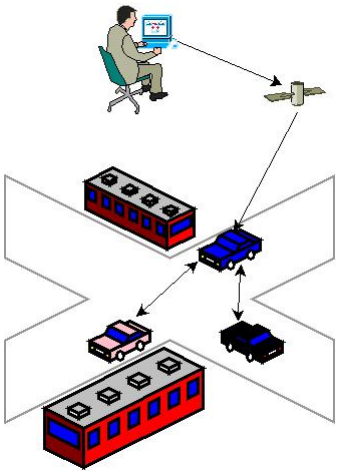

Fig. 2. Remote access to a connected vehicle.

Date: Wed, 30 Jan 2013 11:18:37
From: Admin HDFC Bank <admin.securehdfcbanking@gmail.com>
Reply-To: secure.hdfcinformation@gmail.com
Subject: Survey Request

HDFC BANK

Dear Customer,

You have been selected for our reward survey offer. HDFC Bank values your feedback and is doing a $50 Reward Survey. HDFC Bank will credit your account with $50 after you complete this survey. It will not take more than 5 minutes. To get advantage of this offer and start the survey, click on this link: www.getthisoffer.com/surveyhdfcbank. After completing the survey, reply back with the information specified below within 30 days to receive $50. We will send you a confirmation once you complete the survey and provide your information.

Name:
Address:
Date of Birth:
SSN:
Bank Name:
Bank Account:

This message has been sent only to our special customers. Hurry this offer is open only for next 5 days.

HDFC Bank Survey Department

Fig. 3. Phishing example.

2.2 Demonstration of the limitations of technical security mechanisms

This subsection presents two applications, describes their related digital attacks; and demonstrates the limitations of the technical security solutions for them.

Case 1: Connected vehicle Every (motor) vehicle uses a set of sensors and Electronic Control Units (ECUs) to collect data about the vehicle's behavior and environment, and to control the functionalities of the vehicle. ECUs collaborate by exchanging messages; they compose an in-vehicle network (a.k.a. on-Board network). Motor vehicles, until recently, used to have a closed in-vehicle network, i.e. they did not have external connectivity. Messages exchanged between the components of a vehicle were produced and consumed by the nodes of the in-vehicle network. Today, several applications such as cooperative adaptive cruise control, remote firmware update, e-call, and remote diagnostic of vehicles require communication with the in-vehicle network of the vehicle. A vehicle whose ECUs communicate through an in-vehicle network, and which communicates with neighboring vehicles and Road Side Units (RSUs), personal devices, and Service Centers (SCs) is called a connected vehicle [1]. Figure 2 shows a scenario for remote access to connected vehicles.

In the last decade, several threat analyses, security solutions, and security and privacy architectures have been proposed for assuring secure communication in in-vehicle networks, between vehicles, between vehicles and personal devices, between vehicles and service centers, as well as detecting malicious data, protection against wormhole attacks, secure data aggregation for VANets, use of

devices that include a hardware security module, over-the-air firmware update, protection against denial of service attacks, and access control to applications [1].

Car manufacturers implement security solutions to address the threats. However, there are reports that the security mechanisms they implement are subverted. For instance, Checkoway et al. [24] performed a set of attacks on a vehicle (a sedan) including the following:

A1. Exploit a weakness and a flaw in the authentication program of aqLink protocol implementation, namely, short (8-bits) random numbers and a buffer overflow vulnerability, to upload and run arbitrary code.
A2. Use trojan horse for Android-based smart phones to exploit a buffer overflow vulnerability in the car's hands-free application that uses the Bluetooth protocol. (The attack requires the smart phone to be paired with the car's Bluetooth device.)
A3. Call car and play a well-crafted "song" from an iPad, that exploits a logic flaw and a buffer overflow vulnerability in the authentication of aqLink protocol implementation to upload and run arbitrary code.

These attacks show the limitations of technical security solutions for connected vehicles. For instance, attack scenario A1 exploits an implementation weakness: random numbers are of 8-bits (limitation L2), which allows the attacker to upload an arbitrary program into the embedded system. The code may provide the attacker with the ability to inject messages into the in-vehicle network of the vehicle, such as increasing speed or disabling the brake. The other attack scenarios exploit source code vulnerabilities that the researchers found in the programs of the device: they are new attack scenarios (limitation L3).

Case 2: Online banking Hackers exploit online banking Web application vulnerabilities and user faults through means like social engineering. Social engineering, e.g. phishing attacks, exploit human cognitive biases–creating flaws in human logic using different ways to perceive reality–to trick humans into performing actions, such as disclosing sensitive information. Phishing attacks are conducted through (a) presenting illegitimate digital information that attempts to fraudulently acquire sensitive information, such as login credentials, personal information, or financial information, or (b) masquerading as a trustworthy entity–e.g. a well-known organization or an acquaintance.

The phishing information is usually distributed through emails that contain an attachment, or a web link. Figure 3 shows a phishing email masquerading as HDFC bank.[4] The attack scenarios posed by phishing email include:

B1. Fool online banking users to send the hacker their sensitive information, such as Personally Identifiable Information (PII) and financial information, which could be used for identity theft and financial fraud.
B2. Spoof the bank websites, deceive the users to provide their login credentials, and use the information to hack the users' bank accounts.

[4] HDFC bank is a fictive name.

B3. Deceive users to install malicious software on their computers, which may give the hacker access to the users' computers and other computers accessible from the users' computers or capture their login credentials and personal data and send them to the hacker for malicious use.

Technical and usable security solutions are not sufficient to mitigate attacks B1, B2, and B3. For instance, attack scenario B1 succeeds for users who violate the policy (limitation L1): Banks do not request PII and financial information through emails, so users should not reply to emails requesting such information; attack scenario B2 exploits weak mechanisms (limitation L2) that do not detect Website spoofing; and attack scenario B3 often uses new techniques (limitation L3) to bypass anti-malware software.

3 Usable Security

Whitten and Tygar [25] have identified the weakest link property: attackers need to exploit only a single error, and human frailty provides this error: humans are, frequently, the "weakest link" in the security chain. Whitten and Tygar [25] pointed out that users do not apply security mechanisms, although they know them, simply because the mechanisms are not usable enough. A security software is *usable* [25] if the people who are expected to use it: (1) are reliably made aware of the security tasks they need to perform, (2) are able to figure out how to successfully perform those tasks, (3) don't make dangerous errors, and (4) are sufficiently comfortable with the interface to continue using it.

Security usability addresses the question: why users *can't* apply security mechanisms. The techniques for usable security aim to reduce the complexity of security mechanisms, improve the knowledge of users, and reduce the cost of applying them in terms of efforts and money. However, making security usable and changing users' knowledge doesn't enforce change in their behavior [26]. Sasse and Flechais find that security culture, based on a shared understanding of the importance of security, is the key to achieving desired behavior [26].

4 Overview of Societal Digital Security Culture

Members of the society need to gain knowledge and experience sufficient to **avoid** the consequences of the limitations of technical solutions. Security limitations have been addressed for the case of organizations using DSC, which extends (usable) technical security solutions [21]. The most common definition of DSC–that we adopt in this paper–is the collective knowledge, common practices, and intuitive common behavior about digital security (cf. [19]). This definition identifies knowledge and behavior (which includes practices) as the main levels of DSC.

Table 2 shows the differences between technical security solutions, usable security solutions, DSC and SDSC. It shows that technical security solutions, usable security solutions, and SDSC complement each other, and that SDSC extends DSC from organizations to the society.

Table 2. Difference between the digital security approaches.

	Technical security solutions	**Usable security solutions**	**DSC**	**SDSC**
Target entity	information systems	human-computer interactions	employees in organizations	members of the society
Protection target	information systems and their users	information systems and their users	information systems of organizations	users of the society
Beneficiary	individual	individual	organizations	society
Liability	information system operators	information system operators or distributors	organizations	members of the society, organizations, and law makers.
Preparation for unknown attacks	low	low	moderate	moderate
Technical knowledge requirement	high	low	low	low

SDSC is similar, in principal, to DSC in organizations; it helps individuals use pervasive computing systems, social networks, and public applications while protecting themselves and their assets from digital security threats. Since the limitations of the (usable) technical solutions affect the members of the society in general and an effort at the level of the society should be made to address them, we consider this challenge societal; that is, it does not only concern individuals who happen to be the victims. A second reason for considering the issue societal is the fact that people imitate each others' behaviors.

SDSC and DSC have several differences including the following.

- Organizations decide on the IS they use and can control the threats they are exposed to. In contrast, it is difficult for the society to limit the ISs used by its members–if not impossible.
- Organizations control the selection of their members–so it is possible to select only individuals who share certain values. In contrast, the society has limited control on the selection of the citizens.
- Organizations set the policies for using their ISs. In contrast, the security policies in the society are set in response to events related to using ISs.
- Organizations can set efficient measures for enforcing desired behaviors. In contrast, setting efficient measures for enforcing desired behaviors in the society requires important resources and long time.
- Organizations can easily set measures for detecting violations. In contrast, setting such measures in the society may cause privacy violation. (Recall that members of the society use ISs, in most cases, for private business.)

SDSC of a group has levels which range between weak and strong. Example for indicators of weak SDSC is the willingness of the members of the group

Table 3. Password change habits in the society [27].

	weekly	monthly	twice/year	once/year	never	not sure
How often do you change passwords for your banking account(s)?	8%	16%	19%	18%	28%	12%
How often do you change passwords for your social media account(s)?	6%	11%	13%	19%	42%	10%

Table 4. Generic interest in security [27]

	yes	no	not sure
Does your company have policies/training/security requirements that you must follow when you use your personal device at work?	42%	44%	14%
Have you installed any security software or apps on your smartphone in order to make it more secure from viruses or malware?	31%	64%	5%

to use the pervasive systems without checking associated security risks: potential threats with their occurrence and impacts [28]. Example for indicators of strong SDSC is the importance members of the group give to evaluating the risks associated with a system they intend to use.

A survey conducted in USA in 2012 by the National Cyber Security Alliance (NCSA) and McAfee [27] reveals the weak SDSC in USA. For instance, Table 3 shows that 30% of the interviewees either never or do not recall they ever changed their online banking password (and more than 50% for the case of OSN) and Table 4 shows that about 70% of interviewees are either not sure or did not install a security software for their smart phones.

5 Approaches for Improving Societal Digital Security Culture

This section proposes three approaches for improving SDSC: instituting security policies, spread of knowledge, and behavioral improvement, which are complementary. The approaches are borrowed from DSC in organizations and adapted for society.[5] Table 5 lists the three approaches and the methods that implement these approaches. It specifies for each method whether it affects knowledge and attitude, behavior, or both.

5.1 Institute digital security policies

A digital security policy specifies acceptable and unacceptable behavior in relation to security practices. A collection of security policies specifies, indirectly,

[5] In this section we often use "confer" (cf.) because in the references the ideas apply to organizations; we adapt these ideas to individuals/members of society.

Table 5. Approaches for digital security culture enforcement.

Approach	Knowledge and Attitude	Behavior
Institute security policies		
Develop security policies (P1.1)	x	
Spread the Knowledge		
Security awareness programs (P2.1)	x	
Leadership support (P2.2)	x	
Behavioral improvement		
Use of personal incentives (P3.1)		x
Use of games (P3.2)		x
Use of certification (P3.3)	x	x
Education of children (P3.4)	x	x

the *target SDSC*: DSC that the society wants to "live in." The objective of a security policy is to influence and to direct the behavior of individuals on protecting their own digital assets and themselves (cf. [29]) from security threats to the systems they use and to discourage compromising the security of others.

In order to be a deterrent for attackers and those justifying the abusive use of people's personal information with loopholes in the system, politicians, citizens, and security experts should collaborate to create SDSC in the form of laws. As evident from the aforementioned case study, instituting security policies will not be sufficient for a complete SDSC. The policies need to be (a) disseminated to individuals and (b) enforced through incentives and punishment by laws.

5.2 Spread the knowledge about security threats

This subsection discusses security awareness programs and leadership support as methods that enable spread of knowledge about digital security threats.

Security awareness programs. They aim to improve the awareness of individuals about security risks [30]. They are used to change (and improve) the knowledge and attitude of individuals towards digital security threats. These programs may use (1) promotional methods, such as mugs and screen savers; (2) improving methods, such as rewarding mechanisms; (3) educational and interactive methods, such as demonstrations and training; and (4) informative methods, such as emails and newsletters [31]. Another means of raising security awareness is using OSNs to provide an effective way for information dissemination, especially for educating the public about policies and attacks.

Existing security awareness programs, although successful in changing the attitude toward security risks, are not effective in changing users' habits and intuitive behavior to respond as necessary to security threats [32]. Kruger and Kearney [32] report that trainees exhibit good level of awareness attitudes and knowledge, but exhibit poor security behavior. They report that awareness behavior is as low as 18% when it comes to adhering to the security policies. This shows the limitation of security awareness programs in effectively improving the

intuitive behavior towards security risks, which further supports the use of the suggested approaches to improve SDSC.

Dodge et al. investigated the response of military cadets in USA to the phishing attack [20]. They sent phishing attacks to the students–without previous announcement of the exercise, evaluated the responses, and alerted students about the result of the test. The experiments showed that senior students had better security culture than junior students, which shows the difference between security culture and security awareness.

Leadership support. Leaders support and commitment is crucial to changing SDSC (cf. [33], [29]). Leaders need to embody the security best practices; they should behave according to the policies, be engaged and live up to the security policies they set. The commitment and support of leaders to SDSC change helps disseminate the knowledge because their activities are visible to the society members, which encourage them to, also, practice the policy.

5.3 Improve intuitive behavior towards security threats

This subsection describes four methods for behavior improvement: use of incentives, use of games, use of certification, and use of courses.

Use of personal incentives. *Personal incentives* motivate individuals to change their behavior. They can be categorized in three classes:

- Material or morals rewards: Offering small rewards, e.g., money and praise by peers, to the users to keep them interested in the training program. Thus, over time, they undergo behavioral changes towards perceiving and reacting to the attack scenarios.
- Moral or material sanctions: The fear of embarrassment and punishment, e.g., penalty and blame, forces users to behave appropriately.
- Responsibilities and accountability for complying with policies [29]: Influence the users to be responsible in following the policies. For instance, non-disclosure agreements help preventing leakage of sensitive information.

The effectiveness of rewards and sanctions depends on the satisfaction of the receiving individual [34]. For example, (we expect) a small monetary reward may motivate a poor but not a rich individual.

Use of games. Games are competitive interactions involving chance and imaginary setting and are bound by rules to achieve specified goals that depend on the player skills. By nature, games are competitive; users like to play the games and get better scores. Games could simulate attacks and protection mechanisms.

We propose to exploit the characteristics of games for creating competitiveness to improve SDSC of individuals. Games are already being used in security awareness programs to help employees gain skills to discover threats and develop reactions to them [35]. Users could play a game in which they are required to discover the threats and protect themselves. The games help users understand how to discover threats, know what protection mechanisms are and how they work and how to identify attacks and react to them. They transform the behavior of

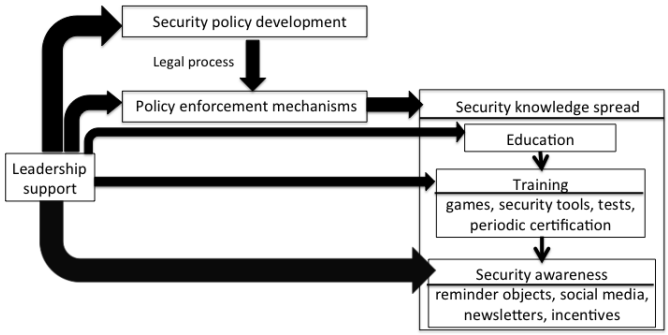

Fig. 4. The SDSC process

individuals from passive, i.e. knowing the impact of the threat, to proactive and engaging, i.e. acting spontaneously to limit the impact of the threat.

Use of certification. Certification of knowledge is important for users handling sensitive information of other entities. It should be made mandatory and enforced by the legal and regulatory policies. Certification can be obtained after completing a certain level of education and training and demonstrating the knowledge through a test. Certifications should require periodic renewal to accommodate updated policies and new threats. For instance, a bank employee handling sensitive financial and user information should renew his/her certification periodically. The certification process enforces the change in user behavior towards securely handling information and prevents attacks.

Education of children. It is very important to introduce children to SDSC when they start using computers and the Internet. Thus, schools need to adopt and offer mandatory classes to teach all children about the SDSC process and its importance. This will help the children easily develop the rightful behavior at an early age when they are just beginning to use digital information systems.

Figure 4 shows how the proposed approaches for improving SDSC should be integrated to achieve a high level of security for any information system. As seen in the figure, while there is a logical time ordering relation between most of the proposed methods, leadership support should come into play at every stage of the SDSC improvement process.

6 Example on Reducing Risks of Security Threats Using Societal Digital Security Culture

This section shows through an example how to improve the SDSC to address phishing attacks. We assume that the online banking system implements usable technical mechanisms and we develop a program that integrates coherently a set of approaches to improve the security culture of a society.

The first phase of the plan is to create two policies (P1.1): (1) no PII should be disclosed through email, and (2) two-step-authentication mechanisms should be required for accounts that use sensitive information (The second step could be providing a secret answer to a personal question in the case that the first step, the login, was performed at a host unregistered by the user). The first policy aims to prevent users from providing sensitive information to hackers, who pretend to be the bank. The second policy aims to prevent users from using a spoofed bank web page requesting login credentials, as the second step of authentication being unique to every user will not match, making the user aware of the phishing attack. The policies–and possibly other policies–should constitute objects of law, created by a government agency, which regulates instituting the policies. The government should enforce the policies.

The next phase is to communicate the policies to members of the society through security awareness programs (P2.1). Users become aware of policies and threats, learn the proper usage of systems and handling of information, develop the behavior to avoid the attacks, and act in case they occur (as they do for the case of a fire for example). The banks could motivate their users by e.g., offering loyalty rewards points (P3.1) for successful completion of training programs and for reporting phishing attacks. The incentives change the behavior of users towards the attack: they would learn to differentiate emails coming from a generic mail service (e.g., Gmail) and emails coming from a bank and recognize phishing email using their characteristics, such as generic greeting, fake sender address, false sense of urgency, and fake and deceptive web links.

Periodic knowledge check through renewable training and certification (P3.3) keeps the users updated about new policies and new threats.

7 Conclusion

The use of pervasive computing systems, social networks, and public information systems exposes individuals to the impacts of security threats to these systems. This paper demonstrates that technical security solutions cannot alone, effectively, protect individuals and their assets from attacks on the systems they use, and proposes to complement (usable) technical solutions with SDSC: collective knowledge, common practices, and intuitive common behavior about digital security that the members of a society share. It also suggests a set of approaches–borrowed from organizational DSC–for improving SDSC.

This work is a first step in investigating SDSC. Our future work will include the development of surveys for assessing the security culture, conduct case studies for improving SDSC (e.g., improve the security culture related to connected vehicles), evaluate the effectiveness of approaches for improving security cultures, investigate how to develop a coherent plan for improving the security culture in a society.

Acknowledgment

This work is supported partially by the Dutch national HTAS innovation program; HTAS being an acronym for High Tech Automotive Systems. Any opinions expressed in this paper are those of the authors and do not necessarily reflect those of Dutch national HTAS innovation program.

The authors thank Drs. Reinier Post and Joost Gabriels from LaQuSo, Eindhoven University of Technology for their valuable comments.

References

1. ben Othmane, L., Weffers, H., Mohamad, M.M., Wolf, M.: A Survey of Security and Privacy in Connected Vehicles. In: Wireless Sensor Networks (WSN) For Vehicular and Space Applications: Architecture and Implementation. Springer, Norwell, MA Accepted.
2. Sundgren, B.: What is a public information system. International Journal of Public Information Systems **1**(1) (2005) 81–99
3. Gilgor, V.: A note on the denial-of-service problem. In: Proceedings of the 1983 IEEE Symposium on Security and Privacy. SP '83, Washington, DC, USA, IEEE Computer Society (1983) 5101–5111
4. Kissel, R.: Glossary of key information security terms. `http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf` (February 2011)
5. Anderson, R.J.: Security Engineering: A Guide to Building Dependable Distributed Systems. 2 edn. Wiley Publishing, Indianapolis, IN (2008)
6. Bailey, D., Solnik, M.: iSEC partners presents: The hacked and the furious. `http://www.youtube.com/watch?v=bNDv00SGb6w` (November 2012)
7. Grebennikov, N.: Keyloggers: How they work and how to detect them (part 1). `http://www.securelist.com/en/analysis/204791931/Keyloggers_How_they_work_and_how_to_detect_them_Part_1` (November 2012)
8. Rosen, J.: The web means the end of forgetting. The New York Times (2010) Published: July 21, 2010.
9. Society, E.I.: ecall: Time saved = lives saved. `http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm` (June 2011)
10. Bosch: Bosch health buddy. `http://www.bosch-telehealth.com/` (January 2013)
11. SGRenovation. `http://sgrenovation.com/why-use-smart-home-appliances/` (January 2013)
12. MyBankTracker. `http://www.mybanktracker.com/news/2010/05/27/` (January 2013)
13. Twitter: Twitter logo. `https://www.twitter.com` (January 2013)
14. Google: Playstore logo. `https://play.google.com/store?hl=en` (January 2013)
15. LinkedIn: Linkedin logo. `http://www.linkedin.com/` (January 2013)
16. Google: Android logo. `http://www.android.com/` (January 2013)
17. Facebook: Facebook logo. `https://www.facebook.com` (January 2013)
18. Skype: Skype logo. `http://beta.skype.com/en/` (January 2013)
19. Williams, P.: What does security culture look like for small organizations? In: 7th Australian Information Security Management Conference, Perth, Australia (December 2009)

20. R. C. Dodge Jr., Carver, C., Ferguson, A.J.: Phishing for user security awareness. Computers & Security **26**(1) (2007) 73 – 80
21. Schlienger, T., Teufel, S.: Information security culture: The socio-cultural dimension in information security management. In: Proc. of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives. SEC '02, Deventer, The Netherlands, The Netherlands, Kluwer, B.V. (2002) 191–202
22. Colella, A., Colombini, C.: Security paradigm in ubiquitous computing. In: Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on, Palermo, Italy (july 2012) 634–638
23. Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T., Maisel, W.H.: Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In: Proceedings of the 2008 IEEE Symposium on Security and Privacy. SP '08, Washington, DC, USA, IEEE Computer Society (2008) 129–142
24. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T.: Comprehensive experimental analyses of automotive attack surfaces. In: Proceedings of the 20th USENIX conference on Security. SEC'11, Berkeley, CA, USA, USENIX Association (2011) 6–6
25. Whitten, A., Tygar, J.D.: Why Johnny can't encrypt: a usability evaluation of pgp 5.0. In: Proceedings of the 8th conference on USENIX Security Symposium - Volume 8. SSYM'99, Washington, D.C. (August 1999) 14–14
26. Sasse, M.A., Flechais, I.: Usable Security: What is it? How do we get it? In: Security and Usability: Designing secure systems that people can use. O'Reilly Books (2005) 13–30
27. NCSA/McAfee: 2012 ncsa/mcafee online safety survey. `http://www.staysafeonline.org/download/datasets/3890/2012_ncsa_mcafee_online_safety_study.pdf` (Oct. 2012)
28. Shirey, R.: Internet Security Glossary, Version 2. RFC 4949 (Informational) (August 2007)
29. Lim, J.S., Ahmad, A., Chang, S., Maynard, S.B.: Embedding information security culture emerging concerns and challenges. In: Pacific Asia Conference on Information Systems, PACIS 2010, Taipei, Taiwan (July 2010)
30. European Network and Information Security Agency: A users' guide: How to raise information security awareness. `http://www.enisa.europa.eu/act/ar/deliverables/2006/ar-guide/en` (June 2006)
31. Johnson, E.C.: Security awareness: switch to a better programme. Network Security **2006**(2) (2006) 15 – 18
32. Kruger, H., Kearney, W.: A prototype for assessing information security awareness. Computers & Security **25**(4) (2006) 289 – 296
33. Lapke, M., Dhillon, G.: Power relationships in information systems security policy formulation and implementation. In: Proc. 16th European Conference on Information Systems, ECIS 2008, Galway, Ireland (June 2008) 1358–1369
34. Pahnila, S., Siponen, M., Mahmood, A.: Employees' behavior towards is security policy compliance. In: Proc. of the 40th Annual Hawaii International Conference on System Sciences. HICSS '07, Washington, DC, USA (2007) 156b–156b
35. Cone, B.D., Irvine, C.E., Thompson, M.F., Nguyen, T.D.: A video game for cyber security training and awareness. Computers & Security **26**(1) (2007) 63 – 72