Empowerment of Health Professionals: How High Level Security Education Can Raise Awareness and Confidence

Matthias HERBST a,1, Christoph BUSCH b, Peter PHAROW c and Bernd BLOBEL c

a Dermatologist, QSD, Darmstadt, Germany
b Fraunhofer IGD, Darmstadt, Germany
c eHealth Competence Center, Regensburg University Hospital, Germany

Abstract. Setting up networks among physicians and other health professionals in virtually any medical discipline is an important part of establishing eHealth worldwide. Medical research strategies nowadays advance diagnostic and therapeutic knowledge and guidelines allowing patients to benefit. Patient data and samples are among the most sensitive information and must carefully be protected according to rules of ethics and professional discretion as well as national and international privacy legislation. A lot has been said about “patient involvement, patient empowerment”. What about health professionals? How can they be involved and empowered to address the paradigm shift towards a personalized health service provision? Information and communication technology (ICT), medical devices, and software applications are not among the topics health professionals typically deal with while being theoretically and practically trained to diagnose diseases and treat patients. An ICT-based training and information provision is required to update the ICT skills of health professionals. The German CAST association provides such an information platform where health professionals attend applied computer security education events. This article aims at describing how ICT and security education is provided to health professionals, and how these training courses are designed, structured, performed, and assessed.

Keywords: ICT, security, awareness, education, training, health professionals

Introduction

Information and communication technology (ICT) is the backbone of companies, research institutions, and the public sector structures. ICT infrastructure is an essential part of the organizational infrastructure as such. More and more, ICT gets important for small business and privateers regardless whether they typically search for reliable information on the Internet, write or receive emails, or use online shops. Any violence of, or attack to, such an ICT may cause unauthorized access to, and modification of, sensitive data, loss of data, loss of availability of services, and loss of respective perform-
ance. Such threats must be analyzed, risks must be validated, countermeasures must be implemented in order to minimize the probability that such situations occur. It’s not only a financial loss; it’s often a loss of reliability, trustworthiness, and creditability.

ICT security is thus of high and even growing importance in virtually any society sector or business domain. But security itself can only be guaranteed in case the responsible parties (user, administrator, chief information officer, IT security officer, data protection and privacy ombudsperson, etc.) are aware of threats and risks, and are keen on identifying and applying countermeasures. This requires awareness, security education, and permanent security training. A slogan that really gets it to the point is “Security is not a product - it’s a process” [1]. It means one can’t buy the perfect security solution just from the stock. Security is a permanent, dynamic process rather than being a static product. Security policies and procedures need to dynamically respond to immediate changes in security infrastructures as such (e.g. new medical devices, applications, updates, upgrades, patches, and migrations) and a related different threat and risk potential caused by the modified ICT environment situation. Advanced education and training is a must to keep even security-aware personnel permanently updated [2].

1. General ICT Security Experience and Expertise Requirements

Healthcare and welfare around the globe in developed countries, developing countries, and countries in transition is turning towards the paradigm of shared care providing an integrated care approach. The underlying paradigm change is bound to an extended communication and cooperation network between different specialized healthcare providers involved in patient’s care. Challenges of increasing quality and related efficiency and efficacy requirements in the respective domains need to be met not only by local and regional providers but increasingly by existing and emerging national and even European networks of healthcare establishments and health professionals.

Advanced health networks including those bridging between persons have to be established and managed from different viewpoints. Legislation and administration needs to be addressed. Another important aspect deals with the domain of technologies with especially the industry and the responsible standards developing organizations (SDO) being in the driver’s seat. Last but not least, the societies shall be addressed by the European Commission, the Member States, and the different stakeholder communities. Special attention needs to be paid to ethics, history, and culture. So networking among stakeholders within and between domains is of growing importance for establishing a stable collaboration and cooperation across national and domain boundaries.

Security requirements in the medical area are technically not that different from other application domains. Apart from a very demanding and dynamic privilege management and access control policy, medical solutions (hospital information systems, public health information systems, radiology information systems, laboratory systems, GP office software, and many other applications) base their security solutions on proper authentication (identification and verification), identity management, confidentiality, integrity, authenticity, availability, and accountability [3], [4].
2. ICT Security Experience and Expertise among Medical Professionals

ICT knowledge and awareness for ICT usage needs to be ranked high in medical professionals’ daily routine. First approaches of a permanent working group called “Quality and Security in the dermatological office” in Germany to improve ICT security in practice were made back in 1993. A list of possible pitfalls was circulated among medical professionals immediately after an accidental distribution of confidential patient data by an ICT service engineer. The following investigation of the case clearly showed that no written service and confidential policy agreements were common in practice up to this time. As a first step, the working group established a mailbox system to distribute important findings regionally to dermatologists. In 1996, this service was integrated into a First Class Server based solution with high level security. This did lead to an intensive discussion on quality and security objectives in medical professionals’ work. In 1998, after having started an intensive cooperation with the German Fraunhofer Institute for Computer Graphics (IGD) and its security experts, the gained experience was integrated as valuable block of knowledge into the in the meantime established Competence Center for Applied Security Technology (CAST) [5].

2.1. Networking and Security Expertise

As of today, most physicians are not really familiar with modern and advanced security technology. The physician’s Internet Service Provider (ISP) is considered responsible for all related security measure. Nevertheless there exists almost no educational proof and no quality test (service certification, quality labeling) to assure that a certain level of experience is guaranteed to be achieved by that service provider. The decentralized location of medical treatment makes it difficult to provide a defined quality region-wide. The forthcoming implementation of Electronic Health Record (EHR) systems and the frequent exchange of sensitive medical data via the open and policy-free Internet make strong and high-level quality and security control measures necessary. Networks of medical professionals start making use of advanced ICT solutions [6].

Telemedicine is more and more being accepted by the medical community worldwide. The secure and reliable exchange of data and images of a patient whose life depends on the correct diagnosis at the right place right in time makes the strongest available security efforts inevitable. The screening of moles in high risk patients, e.g., is a live-long process which makes consequent and secure data storage and exchange absolutely necessary. As a well-known procedure now being applied in medicine as well - the central storage of important data in high security server plants- has to seriously be discussed with all its legal, ethical, and technical advantages and drawbacks. The reliable and liable exchange of administrative and medical (clinical) patient data becomes indeed effective and more reliable by using the much faster DSL technology. Disaster scenarios and emergency concepts are well known in military and civil services all over the world, and have increasingly to be applied in the field of medicine.

Assessment studies and reports on domain-independent security training for domain specialists (like medical professionals) have clearly shown the need for specific education and training concepts comprehensively addressing the domain needs [7], [8].
Permanent training and further education is essential for medical professionals to be aware of both legal requirements and technical solutions for advanced ICT security. To address these aspects, the current eLearning initiative in medicine in general and especially in dermatology was launched about five years ago. Meanwhile, the first course of tele-dermatology concerning the diagnosis of early stages of malignant melanoma is under way. In cooperation with University of Brisbane, Australia [7] and University of Graz, Austria [8], dermatologists from different countries world-wide train the exact and early cancer detection in a course of high level web based education. The Armed Forces Institute of Pathology, USA, uses the Internet for exchanging medical expertise with, and between doctors from all over the world for years [9]. Their seminars are highlights in international pathology diagnosis and learning. International networks and discussion groups are supported by services such as SKYPE [10]. Nevertheless, the contact between patients and their doctors is ameliorated, e.g., by using a calendar of symptoms, by exchanging images and digital photos demonstrating the healing process after surgery, or simply by the coordination of visits in the physician’s office. All these aspects need to be addressed while establishing advanced ICT in the medical domain.

Security is one of the basic principles of modern ICT in medicine. It is a part of the obligatory quality management bases for medical institutions. Therefore all parts of such initiatives should undergo a deep and intensive testing procedure before being rolled out nation-wide. Experience and pitfalls have to seriously be evaluated. The influence of ICT industries and their need to foster effective processes supporting economical interests must not lead to a speedy implementation of unreliable or even insecure technology. Especially an independent forum like CAST is able to independently evaluate best practice procedures for ICT security in medical practices and hospitals to avoid health system collapses by hazardously applied techniques and technologies.

3. The CAST Concept

The Darmstadt-based Competence Center for Applied Security Technology (CAST) was established in 1999 [5]. It aims at bringing security expertise to user communities. One way doing so is a series of workshops. These workshops address a specific security area or topic. Experts introduce recently researched security developments and present their chances and challenges. Intensive discussions with the audience validate requirements and conclusions. In collaboration with the Darmstadt Center for ICT Security (DZI) [11] at the Darmstadt Technical University (TUD) [12], CAST is able to offer a complementary a high-class scientific education and training stream. Within four semesters, ICT employees are entitled to undergo an advanced security course finally awarded with an academic certificate on “ICT Security” after having successfully completed a certain number of academic modules and workshops. CAST and DZI offer this certificate in a joint effort including regular courses at TUD. Specifically designed and developed materials even increase the knowledge on ICT security as course participants are entitled to specific additional training and practice courses. CAST workshops typically provide up-to-date information on hot ICT security topics.

The CAST workshops can meanwhile be considered a backbone of German ICT security education. Workshops typically base on knowledge provided in tutorials, and offer state-of-the art experts knowledge in addressed field of interest. In terms of a
Public Key Infrastructure (PKI), e.g., the tutorial offers basic information about public key (asymmetric) encryption, electronic (digital) signatures, policies, establishment of Trusted Third Party (TTP) services, and advantages / drawbacks of existing and emerging PKI solutions. The workshop itself highlights current technical developments and software / hardware solutions in this domain. Tutorials and related workshops shall be seen as a package thus providing real up-to-date information on the addressed topic.

The list of CAST workshop topics is quite comprehensive and covers application areas ranging from cryptography, biometrics, protocols, privacy, and data protection to security engineering, network security, public key infrastructures, and mobile security. Workshops on security levels and related evaluation as well as on identifying specific security threats complete the spectrum. Complementary workshops address specific business domains like, e.g., security management, electronic payment, identity management, electronic procurement, email, cyber crime, and -last but not least- the medical domain with a yearly MED-CAST workshop. Participants are, e.g., ICT security experts, ICT administrators, ICT managers and decision makers, politicians, end users, SMEs, medical professionals, health professionals, and data protection ombudspersons.

4. The MED-CAST Concept

Medical and health professionals do not spend much time in identifying security threats and risks. Thus, one of the CAST workshops aims at inviting medical professionals and ICT specialists involved in healthcare application development for about 6 years now [5]. MED-CAST addresses different stakeholder groups like people working in healthcare, eHealth experts, ICT employees in healthcare, developers and suppliers of medical devices, security experts, medical and technical safety experts, and many other groups. The number of domain participants is promising (2002: 49, 2003: 61, 2004: 55, 2005: 52, 2006: 32 attendees). The workshop itself consists of 8 to 10 presentations with discussions addressing different aspects of the topic, followed by a panel discussion with an active audience interaction. The feedback is very positive in general.

CAST performs for all workshops an extensive assessment to address awareness and acceptance as well as satisfaction of the attendees and ideas for future events. MED-CAST ranges among the best-assessed workshops. Presentations are evaluated regarding their scientific / educational values and their clarity in presentation. Despite of their basically limited ICT security knowledge, they rated most of the presenters quite high and appreciated workshops as such (for rating details see Figures 1 and 2).

![Figure 1. MED-CAST 2004 Evaluation](image1)

![Figure 2. MED-CAST 2006 Evaluation](image2)

MED-CAST started back in 2002 with an introductory workshop on ICT security aspects in healthcare and welfare. The 2003 workshop addressed infrastructure security
for the medical domain whereas the events in 2004 and 2005 highlighted the importance of secure solutions for applying health cards and health records in Germany and beyond. The 2006 workshop tackled challenges and solutions for secure medical multimedia data storage and exchange including images, audio and video streams. In 2007, the organizers prepared, for the first time at least partly in English language, an event on national security infrastructure experience in Germany and its neighbor countries. The 2008 topic (on April 17th) is related to ICT security in medical imaging.

Over the year educational measures and training courses have increasingly been considered important for medical professionals with speakers from different domains and viewpoints highlighting various exciting new topics of applied security technology in the medical domain. Several field studies concerning the secure transport of visual information were performed meanwhile in cooperation with CAST and IGD.

5. Conclusion

Medical professionals typically have many different tasks others that dealing with ICT security. It’s the treatment of patients that count. So in terms of advanced ICT solutions, they need service providers. But in order to validate and evaluate the quality of the services offered, even medical and health professionals need to have a basic understanding of security and safety in ICT. Threats and risks have at least to be known to them. Awareness of security and safety threats as well as confidence in applied security solutions leads to a higher acceptance level for advanced and secure communication and technical collaboration. The MED-CAST workshops held once a year in Darmstadt have been accepted by the expert community as a forum where speakers from different points of view highlight various exciting new themes and topics of applied security technology. Lots of users and scientists have visited the annual symposia meanwhile. MED-CAST is well established in the domain of health-related advanced applied security knowledge provision. The authors will therefore keep the concept of MED-CAST workshop series running. The 2008 topic is related to ICT security in medical imaging.

Acknowledgement

The authors are in debt to Fraunhofer IGD, CAST as well as their own organizations and partnering experts and associations for their continuous support and cooperation.

References

[7] Peter Hoyer, University Brisbane, AU, status of 2007