CASSIS - Computer-based Academy for Security and Safety in Information Systems

Gernot Goluch, Andreas Ekelhart, Stefan Fenz, Stefan Jakoubi, Bernhard Riedl, Simon Tjoa
Secure Business Austria
Vienna, Austria
goluch, ekelhart, fenz, jakoubi, riedl, tjoa@securityresearch.ac.at

Abstract

Information technologies and society are highly interwoven nowadays, but in both, the private and business sector, users are often not aware of security issues or lack proper security skills. The branch of information technology security is growing constantly but attacks against the vocational sector as well as the personal sector still cause great losses each day. Considering that the end-user is the weakest link of the security chain we aim to raise awareness, regarding IT security, and train and educate IT security skills by establishing a European-wide initiative and framework.

1 Introduction

"*In today's digital age where we live and work, citizens and businesses find Information Communication Technologies (ICTs) invaluable in daily tasks. At the same time, more and more citizens and businesses are at risk of information security breaches.*" [1]

With respect to the statement above, why do we think that ICT is so invaluable in our daily tasks? If you observe the rapid development of the Internet penetration within the last years, it is (definitely not a new but) an undeniable fact that it enables people to communicate and work highly interconnected. According to Eurostat, the European Union average (reference period: first quarter for households, January for enterprises) concerning internet access is that 52% of households and 94% of enterprises are already connected to the internet [2].

There exists a large spectrum of advantages of the internet and its services, which reaches from time-independent communication via e-mails to the comfortable usage of internet banking. Shifting the view from private people to the business sector ICT enabled a more effective and profitable way of doing business than ever imagined before. Keywords like e-commerce, 7/24 availability, internet (trading) portals represent only a fraction amount of companies' possibilities to present and improve themselves within the world-wide connected business world. Private people as well as companies live and operate in a world which is highly dependent on the overall functionality of ICT and absolutely reliant on digital information: "*Dependence on IT continues to grow - only one in six small companies could operate their business without IT.*" [3] Taking medium and large enterprises into account, it can be considered as a fact that they are not able to perform business without continuously functioning ICT. It is exactly this dependency which drives enterprises into a precarious situation where they are absolutely vulnerable to interceptions within ICT usage which is ingrained in daily tasks.

Concurrent to the development of ICT, companies face an increasing number of dangers, including viruses, worms, phishing and social engineering attacks in order to outline the "today's most popular" ones. [3] [4] [5]

Clear and brief, ICT enables a tremendous range of potentials for the private as well as the business sector while concurrently the dependence on ICT increases through the anchorage in daily tasks. Subsequently, interruptions impact daily life enormously. This directly leads to financial and even worse reputation losses. Looking isolated at large enterprises, they may have the budget and the manpower to establish a proper resourced environment in order to secure their ICT and information system (IS) infrastructure. Taking small and medium enterprises into account, at least financial considerations let security issues often take a back seat. Focusing purely on securing the IT landscape, there exist various security techniques for securing a company's valuable assets.

[3] [4] [5] show that anti-virus software and firewalls are common used techniques. This is a good basis, but definitely only half the way of securing business. "*When trusted employees are deceived, influenced, or manipulated into revealing sensitive information, or performing actions that create a security hole for the attacker to slip through, no technology in the world can protect a business.*" [6] At the

latest, we now have to leave the isolated technical ICT and IS point of view behind us and turn towards those resources which business is fundamentally dependent on: employees, human beings.

As a basis for further discussions, following statement of Bruce Schneier provides a good fundament: "*...concluding that employees don't care about security is a bit naive. Employees care about security; they just don't understand it. Computer and network security is complicated and confusing, and unless you're technologically inclined, you're just not going to have an intuitive feel for what's appropriate and what's a security risk. Even worse, technology changes quickly, and any security intuition an employee has is likely to be out of date within a short time.*" [7]

As outlined above, the weakest link of the security chain is an employee which is either not aware of security issues or does not own the proper security skills to fulfill its duty accountable. In order to "fill the gap" between the employee that cares per se about his work and his lack of security awareness and knowledge, we established the project CASSIS approach to address the specific needs of employees which is the basis for protecting business.

2 Related Work

2.1 E-Learning

"*We want to do more to exploit the educational potential of new technologies. ... And we must keep the curriculum moving, to take advantage of new methods in all subject areas, and to keep demanding a better response from the technology.*" [8]

Further-on the succeeding definitions of the term e-learning are taken into consideration when defining the CASSIS e-learning approach and architecture.

The Higher Education Funding Council has adopted a fairly liberal view of e-learning in order not to "*curb exploration and restrict diversity*" but to ensure the "*confident use of the full range of pedagogic opportunities provided by ICT, including its use ... as a communications and delivery tool between individuals and groups, to support students and improve the management of learning*" [9]. Following British Educational Communications and Technology Agency, "*E-learning exploits interactive technologies and communication systems to improve the learning experiences. If someone is learning in a way that uses information and communication technologies (ICTs), they are using e-learning*" [10]. The European Commission Action Plan for designing tomorrow's education defines it as, "*the use of new multimedia technologies and the Internet to improve the quality of learning by facilitating access to resources and services as well as remote exchanges and collaboration*" [11].

2.2 Laboratories

New technologies like simulated and remote computing changed the laboratory education landscape [12] by increasing the reach of pedagogy resulting from to the overcome of geographically distances. In contrast those techniques may remove insights associated with traditional laboratory learning [13]. Current research focuses, besides the classic hands-on laboratory approach, on two new technology-intensive automations: simulated labs [14] and remote labs [15, 16, 17]. Due to the major role of laboratories in the CASSIS project we will discuss the shortcomings and advantages in the following.

Hands-On: Hands-on laboratories include two characteristics distinguishing it from simulated and remote labs: (1) physically set up equipment and (2) physically present students. The most important advantage of hands-on labs concludes from the provision of real data and "unexpected clashes"; thus taking into account the disparity between theory and practical experiments [13]. Such experiences for students are missing in simulated labs [18]. Disadvantages result from high needs regarding space, instructor time, and experimental infrastructure; all leading to rising costs [19]. Due to the limitation of resources, hands-on labs are also incapable of meeting special needs regarding disabled students [20] or distant users [21].

Simulated: Simulated labs imitate real experiments by replacing the required infrastructure and resources through simulated images on the computer. Among the major advantages, cost-efficiency and effectiveness through an active mode of learning are prominent factors. Using simulated labs "students ... are able to 'stop the world' and 'step outside' of the simulated process to review and understand it better" [22]. Subsequently simulate labs are seen as being at least as effective as classic hands-on labs. Disadvantages derive from the excessive exposure to simulation, resulting in a disconnection between the real and the simulated environment [18]. Additionally, realistic and complex simulations need enormous amounts of resources in development, reducing the cost-efficiency advantage drastically.

Remote: Similar to hands-on labs, remote labs require physically set up equipment. The main difference concludes from the distance between the course conducted in the lab session, and the participating students. Furthermore remote labs are becoming more and more popular [23]. A remote laboratory extends the capability of classic hands-on laboratories by increasing the flexibility a course can be performed [17]. Disadvantages can arise from the fact that students may not consider remote labs realistic, therefore removing the differences between simulated and remote labs, and denying the fact that real data is provided [24].

3 CASSIS Aim

Figure 1 shows schematically the goals of CASSIS which are succeedingly described in detail.

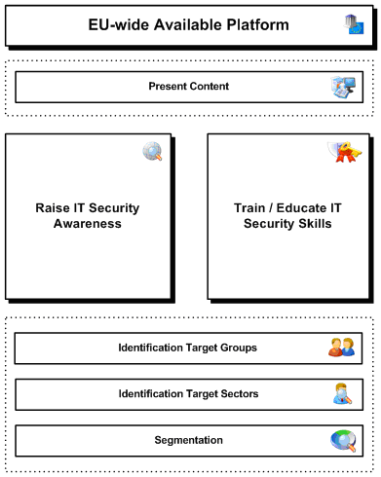

Figure 1. CASSIS Pillars

The overall aim of CASSIS is the generation of an European-wide network of security institutions that establish a multi lingual e-learning platform and training environment in order to raise security awareness and train and educate IT security skills. As a basis for training and education of IT security skills we plan to provide an awareness campaign which is based upon of best practices and guidelines, i.e. ENISA [1] or NIST [25]. Regarding training and education in the field of IT security we define three objectives: Firstly, we generate theoretical security content out of the partners' expert knowledge. Afterwards we translate the gathered knowledge into different languages and present it using multiple channels customized to the preferences of the user. Secondly, we create training labs to communicate the results of the preceding step. Thirdly, we aim at establishing a security community which autonomously supports users regarding their IT security concerns. Finally, we provide a guide how to extend the CASSIS framework, respectively system, with new learning content to ensure the continuous operation of the platform and community.

4 The CASSIS Approach

As presented before the ambitious goal of CASSIS is to increase the skills and awareness of employees in security. Within the following chapters, we introduce our approach by concentrating on the fundaments and main modules of the planned CASSIS architecture.

4.1 CASSIS Knowledge Management

The specific knowledge management approach for our project is based on the building blocks of Probst [26]. This model consists of the following eight building blocks:

1. *Knowledge Goals*: The knowledge goals outline which knowledge needs exist. The goals can be split into normative, strategic and operational knowledge goals.

2. *Knowledge Identification*: A very important factor before starting the development of new capabilities is the identification of existing knowledge. This can be supported by increasing the knowledge transparency (i.e. Knowledge maps).

3. *Knowledge Acquisition*: Knowledge management often requires resources which are not available in the company. Therefore it is often necessary to acquire knowledge of other parties (i.e. Experts, Knowledge products).

4. *Knowledge Development*: This component consists of all activities which create new knowledge. According to Probst knowledge development can be categorized into individual and collective knowledge development.

5. *Knowledge Distribution*: Knowledge distribution supports the efficient exchange of knowledge. This stage is one of the most challenging because the distribution must fit the user needs.

6. *Knowledge Preservation*: This stage deals with the question how to preserve the knowledge of the parties concerned.

7. *Knowledge Use*: The key point within this phase is that the user must see his advantage of the new knowledge and adopt his behaviour according to the gained skills.

8. *Knowledge Measurement*: The measurement and evaluation provides an enormous challenge because it is very difficult to measure the value of knowledge management.

4.2 Evaluation Criteria Selection

The aim of the criteria selection is to determine the main characteristics of CASSIS' goals. It is essential to pay special attention to obtain measurable criteria in order to enable proper evaluations, i.e. 1 Million users within the first two years after the CASSIS framework has been established.

CASSIS will be established through various subprojects, evaluation criteria for each subproject as well as the overall project goals has to be determined. The degree

of the selected criteria's accomplishment reflects the degree of project success. According to Jenny [27], a project is successful if the intended results can be achieved with the planned funds, within the defined temporal scope and within the aimed quality.

4.3 Target Sector & Group Identification

During our research activities we have identified three target sectors and various corresponding target groups (see figure 2) based on the corresponding categorization ENISA awareness guide [1]. All sectors share a knowledge basis which comprises general theoretical IT security knowledge and related practical learning modules which have to be understood before sector specific content is provided to the trainee. The next layer covers our target sectors: personal, vocational and educational. Each of these sectors offers specific but non-exclusive knowledge and content presentation. One layer above, we concentrate on the needs of selected target groups within the target sectors, such as parents in the personal or health in the vocational sector. In the following chapters, the target sectors and related target groups are explained in detail.

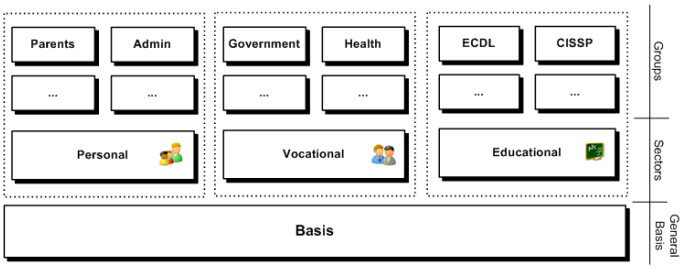

Figure 2. CASSIS Target Sectors & Groups

4.4 Target Sector & Group Analysis

4.4.1 Personal Sector

Direct fraud losses from online phishing scams in the UK almost doubled in 2005 to 23.2 Million pounds, according to statistics from the Association for Payment Clearing Services (Apacs) [28]. Phishing attacks are based on the nescience of users and attempt to fraudulently acquire sensitive information, for instance passwords and credit card details. Social attacks can be avoided by raising awareness, regarding IT security specifics concentrating on users of services. The personal sector covers a broad field of IT security knowledge and exercises which are relevant for the target audience from kids to seniors or rookies to experts.

Defining the personal sector within CASSIS, it summarizes all activities not conducted or supported by an organization excluding concrete educational activities provided by the educational sector.

Table 1. Content/Visualization - Personal Target Sector - Overview

Know-How / Age	6 to 10	11 to 15	16 to 64	64+
low	x	x	x	x
medium		x	x	x
high			x	

Table 2. Content/Visualization - Personal Target Sector - Detail

Age/Knowledge	Content	Profile
6 to 10 / low	General Basics, Awareness	Kid
11 to 15 / low	General Basics, Awareness	Teenager
11 to 15 / medium	Applied IT security, Awareness	Teenager
16 to 64 / low	General Basics, Awareness	Adult
16 to 64 / medium	Applied IT security, Awareness	Adult
16 to 64 / high	Advanced IT security	Adult
64+ / low	General Basics, Awareness	Senior
64+ / medium	Applied IT security, Awareness	Senior

Classification-Schema: Within the personal sector, we identified two important classification characteristics: (1) IT security knowledge and (2) age. Based on this classification schema, we created twelve different sub-target sectors differing in the two classification characteristics. To achieve an efficient coverage of EU-citizens we decided to focus on specific sub-target sectors, excluding those which are unlikely to present an adequate amount of users or a sufficient need for the framework's content, i.e. kids between six to ten holding high IT security skills. The covered sub-target sectors are marked within table 1.

The content and visualization profile has to be optimized for each sub-target sector. Thus, we created the following content- and visualization-profiles.

Depending on the given IT security knowledge described in table 2, different learning content will be presented to the user.

Visualization Profiles

- *Kid:* A playful layout is required for this profile. Text should be used very sparely; instead animations, pictures and comic strips should illustrate the IT security knowledge. The terminology of the text has to be adequate for children in the age of 6 to 10 years.

- *Teenager:* The teenager profile represents the IT security content in a playful way which is suitable to obtain the attention from 11 to 16 year old teenagers. Animations and figures have to be designed in a hip way and the used terminology contains simple terms of the IT security field. Sample videos provide the target group with concrete knowledge, for example about how to manipulate operating system settings.
- *Adult:* The layout has to be designed in a neutral and appealing way; animations are designed with the goal to maximize the knowledge transfer. The biggest part of the learning content has to be communicated by textual descriptions and corresponding figures. Sample videos provide the target group with concrete knowledge about for example how to manipulate operating system settings.
- *Senior:* The senior profile pays attention to the accessibility of the learning content and optimizes the content representation for people with an age greater than 64 years. Like the adult profile the senior profile uses mainly textual descriptions, figures and sample videos to communicate the content. To enhance the readability we will use adequate font and figure sizes. Navigational buttons as well as links will be properly designed.

Target Groups

- *Parents:* The world wide web and computer world in general can be a dangerous place for children; at the moment campaigns around the world try to call attention on this fact [29] [30] [31]. Realizing the danger is an important point but not sufficient enough, parents also need the knowledge on how to control and support their children, regarding the practical use and aspects of information technology.
- *Home Administrators:* More and more households conduct private networks, including wireless technology which demands particular IT security measures and settings. Securing such an environment is a non-trivial task and deficiencies can cause serious damages: e.g. eavesdropping of private information, non-authorized bandwidth usage from outsiders, etc.

4.4.2 Vocational Sector

In 2005, the financial loss caused by malicious code was estimated to exceed 14 billion US dollars [32] and it is expected that the distribution of malware will continue to grow in the future [33]. Malicious code itself is not able to cause this loss, mostly a user is the weakest point in this chain. Therefore it is important to raise the awareness of all actors within companies to counteract these threats. Besides malicious code prevention we also cover the general understanding of IT security to ensure due diligence and business continuity.

Table 3. Content/Visualization - Vocational Target Sector - Overview Business View / Organization Category

Bus. View / Organization	micro	small	medium	large
IT-Management	x	x		
Business Management	x	x	x	
Employee	x	x	x	x

Defining the vocational sector within CASSIS, it summarizes all activities conducted or supported by an organization excluding concrete educational activities provided by the educational sector.

Classification-Schema: Within the vocational sector we identified three important views: the IT management, the business management and the employee view. In consideration of the organization size, we created the following sub-target sectors (relevant sectors are marked) (see table 3).

According to the SME definition of the european commission [34] micro-sized organizations have less than ten, small-sized organizations less than 50 and medium-sized organizations less than 250 employees. Organizations with more than or equal to 250 employees are categorized as large organizations. Besides the organization category we considered the IT management, the business management and the employee view to cover the different needs. The IT-Management view of medium- and large-sized organizations and the Business Management view of large organizations will not be in the main focus of the CASSIS project, due to the existing enhanced IT security awareness and knowledge of these roles in such corporations.

Visualization Profiles

- *IT Management View:* The IT management is responsible for the implementation and maintenance of the IT infrastructure. "*Technically inclined, this group of users may not be security experts, but need to understand and implement information security protocols.*" [1] Practical aspects of IT security such as network security and access control are covered in this CASSIS domain.
- *Business Management View:* The business management is responsible for strategic and organizational aspects concerning the implementation of IT security. "Often not technically orientated, this group of users needs to be educated and understand the importance

of information security." [1] This will allow them to implement the relevant security policies and controls in their business areas. Furthermore knowledge on IT security standards such as ISO17799 [35] and CobiT [36] are included in this program module.

- *Employee View:* Employees represent the largest number of users within the target sector and arguably the most important group [1]. As research suggests, most of the information security breaches in organizations are caused by human error. Thus, we provide thorough education regarding IT security awareness and correct IT infrastructure handling.

Target Groups

- *Government:* Governments operate on sensitive data and therefore have high standards regarding IT security. CASSIS aims to support government employees in their daily tasks, to raise their awareness and teach practical and applied aspects of IT security.
- *Health*: Confidentiality and privacy is of high importance in the health sector. People working in this area have to be aware of how to handle data concerning privacy of personalized information and country-specific law.

4.4.3 Educational Sector

Defining the educational sector within CASSIS, it comprises specific educational programs such as the CISSP certification or a future IT security ECDL program. These educational programs can be attended by individuals from the personal or vocational sector with the goal to be optimal prepared for the subsequent certification exams.

4.5 Content Identification and Selection

Experts agree [37] that the identification and assignment of learning modules, according to the needs of a user, are by far the most difficult challenge when launching an e-learning platform. The special challenge is to present the right content in the right way. Several aspects like motivation, skills, age and profession have to be taken into account in order to determine the right selection for the user. Due to the wide range of users' motivations and interests, it is important to involve a huge variety of experts into the project.

Therefore the committee carefully selects the learning content with respect to the user groups and motivation described above. This committee consists of several experts in the field of IT security, e-learning, education and sociology on the one side and representatives of users on the other side. We think it is exactly this combination of expertise which assures that the content is presented to the target group via those media which fits the users' needs. After the experts agreed on several learning modules, we define evaluation criteria and prototype learning packages for lab use. Succeedingly, we perform a first evaluation to assure the quality of the content and presentation.

The CASSIS project group intends to generate this learning content according to the pattern of reusable learning objects. We decided to use this concept to support the use of learning management systems. To reach the goal of reuse, the metadata of these components has to be described in a standardized way like learning object metadata [38], the IMS metadata specification [39] or the ISO/IEC JTC1 [40]. This ensures that the content generated for this platform can be exchanged amongst others.

4.6 Security Software Learning Packages - Laboratories

Laboratory-based experiments and courses hold a major role in education: Experts claim that "*hands-on experience is at the heart of science learning*" [41]. Due to the fact that learning in such laboratory environments has a strong positive impact on the specific learning outcome of users [42], we focus strongly on the development of practical learning packages, which can be used in hands-on, simulated and remote laboratories.

The user can utilize the offered learning packages in a three folded way: (1) he can read and study the content (text & optionally sound), (2) then he is able to watch the practical exercises and (3) he can try to solve the presented problem(s) and/or exercises by himself using a testing environment. The usage of the presented practical tests are optimized for hands-on, remote and simulated learning experience. The user has the possibility to be lectured in a class, in a virtual class or by himself and to be tested within a physical, a simulated and a geographically distant laboratory.

4.7 CASSIS Platform

The proposed CASSIS framework, depicted in figure 3, comprises the following modules: The CASSIS knowledge base contains basic knowledge modules such as "data recovery & backup" and "network & internet security". We establish the CASSIS learning content management system (CASSIS-LCMS) which enables centralized management and reuse of all learning content. "*LCMS is a system (mostly web-based) that is used to author, approve, publish, and manage learning content (more specifically referred to as learning objects).*" [43] The CASSIS content presentation layer prepares the content from the CASSIS LCMS in a way which is suitable to transfer the content over a specific channel to the user. We propose the channels internet

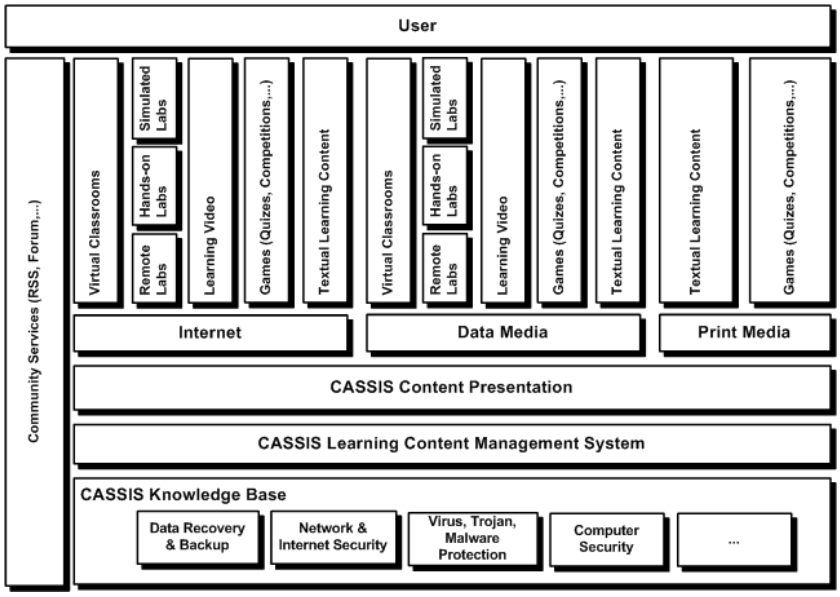

Figure 3. CASSIS Framework - Architecture

(website, newsletter,), data media (CDs, DVDs, USB-stick,) and print media for the distribution of the learning content. Depending on the used channel we propose the following knowledge transfer approaches (1 Virtual Classrooms: Moderated software-supported learning unit, (2) Remote, Hands-on and Simulated Labs (see section F), (3) Learning Video: Video presentation of the learning content, (4) Games: The learning content is taught in a playful way to the user and (5) Textual Learning Content: Textual presentation of the learning content including figures to enhance the clarity. The entire CASSIS framework is flanked by community services such as RSS feeds and a forum for user exchange. The top layer represents the actual user who consumes the services of the CASSIS framework.

4.8 CASSIS Product Life Cycle

As CASSIS' product is information, we established a concept for the CASSIS-specific information product life cycle approach. Within our concept we aim at two different life cycles, one for the first and the other for all subsequent iterations. The first life cycle represents a traditional product life cycle [44], schematically shown in figure 4 ("First iteration" curve). Due to the fact that CASISS is not a product which aims at revenues, we interpret revenue not in cash but in the usage of the framework. The introduction stage is the most expensive stage with the lowest revenue growth. Within the growth stage we estimate a considerable revenue increase while the expenses are further on high, for example caused by necessary marketing investments. Concerning the maturity stage, we expect a deceleration of growth

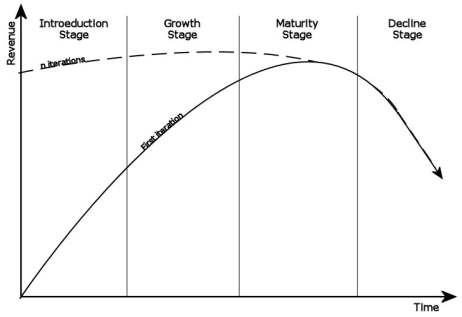

Figure 4. CASSIS Product Life Cycle

and a respectable penetration of our target groups' "market". At this point, evaluations within the previous stages lead to a modification of the CASISS framework as well as the presented information and content which effects directly on our second life cycle concept. The decline stage is the last phase of the life cycle which we want to "skip" through our second life cycle concept, schematically presented in figure 4 ("n iterations" curve).

The second life cycle concept is applicable for all life cycle iterations but the first one described above. Due to the evaluation (per iteration) of the life cycle before the actual one, we aim at shifting the first life cycle curve to minimize the costs while maximizing the revenue through the continuous modification and updating of the presented information and content. Within the introduction stage the incurred expenses of deploying the modified versions are comparatively low to the added value of the evaluated updates. The curve within the growth stage of the iterations is

gently inclining in comparison to the first iteration curve's gradient. This is caused by our estimates that the largest increase in revenues happens within the first life cycle iteration. Reaching the maturity stage, evaluations will again be performed in order to trigger the next modifications and life cycle iteration.

With our CASSIS life cycle concept we firstly aim at mitigating the usual impacts of each decline stage and secondly, on a continuous advancement of the CASSIS framework and its most valuable product: its information. Further research has to be done to identify the optimum point in time of launching new life cycle iterations (impact mitigation). Furthermore, we have to investigate the most proper strategy of modifying and updating the evaluated information. At the current state, we consider an open source approach what would lead to a strong interaction with the CASSIS community. Another approach we have to investigate carefully is the establishment of a commercial alternative in order to fund CASSIS own employees.

5 Conclusions and Further Work

We proposed the "Computer-based Academy for Security and Safety in Information Systems" (CASSIS) approach for an IT security specific e-learning architecture, respectively system. Components, like the knowledge management module, practical learning packages, the platform architecture itself and our dissemination plan regarding the product life cycle were presented. At our current state of research we concentrate on deliverables for the domains of malware, fraud, privacy, trust, social engineering and legal issues. Further-on we plan to propose this project in the european Leonardo funding program, concentrating on vocational education and training in IT security, which should enable us to implement and create the presented approach in together with several european partners (e.g. ENISA, University of Malaga, University of Regensburg, Technical University of Vienna).

6 Acknowledgements

This work was performed at Secure Business Austria, a competence center that is funded by the Austrian Federal Ministry of Economics and Labor (BMWA) as well as by the provincial government of Vienna.

References

[1] ENISA, "A users guide how to raise information security awareness," http://www.enisa.eu.int/doc/pdf/ deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf, 2006.

[2] Eurostat, "in the eu25, eurostat news release 146/2006," 2006.

[3] PWC/DTI, "Information security breaches survey," 2006.

[4] CSI/FBI, "Computer crime and security survey," 2006.

[5] AusCERT, "Computer crime and security survey," 2006.

[6] K. Mitnick, *The Art of Deception*. John Wiley & Sons, 2002.

[7] Schneier, "Proof that that employees don't care about security," Blog, February 2006, 2006.

[8] DfES, "Department for education and skills: Harnessing technology: Transforming learning and childrens services." http://www.dfes.gov.uk/publications/e-strategy/ Accessed 29.10.2006, 2005.

[9] HEFCE, "Higher education funding council: Hefce strategy for e-learning," http://www.hefce.ac.uk/pubs/hefce/2005/05_12/ ACCESSED 29.10.2006, 2005.

[10] B. E. Communications and T. Agency, "Open source software in schools: A case study report," http://becta.org.uk/, 2005.

[11] E. Commission, "The e-learning action plan; designing tomorrows education." 2001.

[12] E. Scanlon, E. Morris, T. D. Paolo, and M. .Cooper, "Contemporary approaches to learning science: Technologically-mediated practical work." *Studies in Science Education*, vol. 38, pp. 73–114, 2002.

[13] J. Ma and J. Nickerson, "Hands-on, simulated, and rmote laboratories: A comparative literature review," *ACM Computing Surveys*, vol. 38, pp. 1–24, 2006.

[14] E. McAteer, D. Neil, N. Barr, M. Brown, S. Draper, and F. Henderson, "Simulation software in a life sciences practical laboratory," *Computers and Education*, vol. 26, pp. 101–112, 1996.

[15] M. Aburdene, E. Mastascusa, and R. Massengale, "A proposal for a remotely shared control systems laboratory," in *In Proceedings of the Frontiers in Education 21st Annual Conference*, 1991.

[16] M. Albu, K. Holbert, G. Heydt, S. Grigorescu, and V. Trusca, "Embedding remote experimentation in power engineering education," *IEEE Transactions on Power Systems*, vol. 19, pp. 139– 143, 2004.

[17] G. Canfora, P. Daponte, and S. Rapuano, "Remotely accessible laboratory for electronic measurement teaching," *Computer Standards & Interfaces*, vol. 26, pp. 489–499, 2004.

[18] D. Magin and S. Kanapathipillai, "Engineering students' understanding of the role of experimentation," *European journal of engineering education*, vol. 25, pp. 351–358, 2000.

[19] P. Farrington, S. Messimer, and B. Schroder, "Simulation and undergraduate engineering education: The technology reinvestment project (trp)," in *In Proceedings of the 1994 Winter Simulation Conference*, 1994.

[20] C. Colwell, E. Scanlon, and M. Cooper, "Using remote laboratories to extend access to science and engineering," *Comput. Educ.*, vol. 38, no. 1-3, pp. 65–76, 2002.

[21] H. Shen, Z. Xu, B. Dalager, V. Kristiansen, O. Strom, M. Shur, T. Fjeldly, L. Jian-Qiang, and T. Ytterdal, "Conducting laboratory experiments over the internet," *IEEE Transactions on Education*, vol. 42, pp. 180–185, 1999.

[22] A. Parush, H. Hamm, and A. Shtub, "Learning histories in simulation-based teaching: the effects on self-learning and transfer." *Computers and Education*, vol. 39, pp. 319–332, 2002.

[23] S. Yoo and S. Hovis, "Technical symposium on computer science education." in *In Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education.*, 2004.

[24] Z. Nedic, J. Machotka, and A. Nafalski, "Remote laboratories versus virtual and real laboratories." in *In Proceedings of the 2003 33rd Annual Frontiers in Education Conference.*, 2003.

[25] NIST, http://csrc.nist.gov/, 2003.

[26] G. Probst, "Practical knowledge management," Prism, Arthur D Little, 1998.

[27] B. Jenny, *Projektmanagement in der Wirtschaftsinformatik. 5. Auflage*. Hochschulverlag AG an der ETH Zrich, 2001.

[28] URL, http://www.finextra.com/fullstory.asp?id=15013, 2006.

[29] ProPK and FSM, "Polizeilichen kriminalprvention der lnder und des bundes (propk), der freiwilligen selbstkontrolle multimedia (fsm): Kinder sicher im netz," http://www.polizei-beratung.de/vorbeugung/medienkompetenz/internet/, 2006.

[30] ORF, "ffenltich rechtlicher rundfunk sterreich: Sehen sie, was ihr kind sieht?!" http://jugendschutz.orf.at/, 2006.

[31] EU, "Europe's internet safety portal," http://www.saferinternet.org/, 2006.

[32] C. Economics, "Malware report:the impact of malicious code attacks," 2005.

[33] Symantec, "Internet security threat report: Volume x," 2006.

[34] URL, http://ec.europa.eu/enterprise/enterprise_policy/sme_definition, 2006.

[35] "Iso17799," http://www.iso.org/, 2006.

[36] "Cobit," http://www.isaca.org/, 2006.

[37] J. Liu and J. Greer, "Individualized selection of learning object," in *International Workshop on Applications of Semantic Web Technologies for E-Learning*, 2004.

[38] LTSC-IEEE, "Learning technology standards committee ieee: Draft standard for learning object metadata," http://ltsc.ieee.org/wg12/files/LOM_1484_12_1_v1_Final_Draft.pdf, 2002.

[39] IMS, "Ims metadata specification," http://www.imsglobal.org/metadata/, 2002.

[40] ISO/IEC, "Working draft for iso/iec 19788-2 metadata for learning resources," http://mdlet.jtc1sc36.org/doc/SC36_WG4_N0145.pdf, 2005.

[41] N. Nersessian, "Conceptual change in science and in science education." in *In History, Philosophy, and Science Teaching*, 1991.

[42] D. Magin, A. Churches, and J. Reizes, "Design and experimentation in undergraduate mechanical engineering." in *In Proceedings of a Conference on Teaching Engineering Designers.*, 1986.

[43] M. Nichani, http://www.elearningpost.com/articles/archives/lcms_lms_cms_rlos/, 2001.

[44] H. Reisinger, K. Srnka, and M. Heindler, "Online marketing lexikon," http://www.univie.ac.at/marketing/Lexikon/beg/plc.htm, December 2006.