Fulfilling the Needs for Information Security Awareness and Learning in Information Society

Juhani Anttila
Quality Integration, Finland

Reijo Savola
VTT Technical Research Centre of Finland, Finland

Jorma Kajava
University of Lapland, Finland

Juha Lindfors
University of Lapland, Finland

Juha Röning
University of Oulu, Finland

Abstract

In information society and business world, there are different levels of needs for information security awareness and learning, e.g. the needs for ordinary citizens, business leaders, and experts. Users of information systems – factually all members of society – should have at least basic literacy of information security. In the day-to-day business life, advanced skills of information security awareness are needed by business managers. At the expert level, the developers of technical and organizational solutions for the Information and Communication Technology (ICT) need to have a wide understanding of information security threats and opportunities and related solutions. Information security officers or managers have a key role in organizations in developing and maintaining their organizations’ systematic approach of information security according to the organizations’ business needs. It is essential that the learning methodologies can answer to the needs of all different actors in society. In this paper, we analyze these needs and the type and contents of learning needed and consider the development in training, education and learning from traditional approaches to new challenges.

Keywords: information security education, information security awareness
1 Introduction

ICT is aimed at helping our lives and making the society more in efficient in its services. Ever more powerful personal computers and other personal digital assistants, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross organizational and national borders. In addition, the Internet supports critical infrastructures of society and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information (OECD, 2000).

The development has been rapid and there are still quite a lot of challenges in coping with the new situation. However, the development has not been without troubles. The development and use of the ICT solutions has often been problematic (Collins, 2001). Many new ICT applications have also made the jobs of people more complex and difficult. This includes problems for employees and business leaders making operational and strategic decisions, and because they have to access many ICT applications to do their jobs. In many cases the data sources, systems, and applications located throughout the organization need to be combined to present the summarized information for business needs. Corporate-wide systems are complex and designed for a specific purpose and function, so the ICT department is required to deploy many different and often unrelated applications and modules to fill the information and processing needs of the entire organization. An incredible amount of training time is needed for employees to learn how to use effectively such a complex applications to complete their assigned responsibilities. These complexities have also harmful impacts to information security.

We get more challenges also because the whole nature of ICT is changing and becoming more multi-faceted. Some people have given a new interpretation to the concept ICT, Interactive Collaborative Technology.

Today’s dynamic business environments are characterized by continuous changes and effects of global interactive independent actors especially involving competing or conflicting political, social, and psychological factors. This breeds many difficulties for realizing information security management in a professional way but it also gives very new possibilities related to new technological and collaborative tools for managing information security if only the foundations of the new business behaviours are understood deeply (Locke et al, 2000).

Organizations in the networked business environments are heterogeneous, and the local rules organize their interaction. Key concepts are self-organization and emergence. Organizations are interacting in networks by complex responsive processes of relating (Stacey, 2002). In this situation it is better to use the term active processes rather than to talk about passive organizational systems, e.g. information security systems. Central to these complex responsive processes of relating are communicative interactions among people.
Information security and privacy are remarkable challenges for organizations and the society at large. Because of the speed of the development, information security and privacy solutions are not always at adequate level. In the process of making an information security aware society happen, we need understanding, knowledge, and learning on information security through the whole society. However, the needs of different actor groups are different. In this text, three significant actor categories are considered, general population i.e. ordinary citizens, business people and particularly business leaders, and experts of information security and related areas.

Information security awareness is here also reflected on its deepness point of view. Increasing awareness equals with enhancing understanding and learning clarified principles, and new skills and practices among individuals and communities. Earlier learning was mainly achieved through training and education activities, e.g. courses, programs, etc. that are nowadays also carried out by e-learning systems and facilities. However, these traditional practices are not enough for deep awareness and have not proved really effective. Only very basic knowledge of information security may be provided by traditional training and education means. Application of new learning theories and innovations of networked interactive information technology give promising views also for learning in information security.

2 Needs for Information Security Knowledge

In the following, we discuss the needs for information security knowledge from different perspectives: general population, organizational management and information security experts and professionals.

2.1 Basic Information Security Literacy for the General Population

Many functions of our information society are already now depending on information and communication technologies. For example, electronic services can be used in carrying out government procedures such as revenue services, employment services or voting and also for shopping and paying. This results to a situation where citizens and members of the society should be security aware to the necessary extent. End users are using ICT services both in their private life and also in their working environments in different organizations. In fact, we can say that end user security awareness is one of the most important security issues in our society. The citizens should have at least basic literacy of information security. The most important issues in the basic literacy of information security include understanding and deployment of:

- Deliberative ability when using computer networks and critical information or authentication tokens
- Observance of rules in cyberspace as in the traditional society
- Self-protection, especially in privacy-sensitive situations
2.2 Managing Organizations with Regards to Information Security

Information security competence is needed in all fields of business life in both companies and public organizations. It is important to understand information security holistically and apply this to everybody’s own work. Floor level employees need the basic information security skills and awareness how those skills are really applied in their particular organizations and business activities. They should clearly understand organization’s security policy in general and particularly in their own working contexts.

Especially senior executives are responsible of managing organizations with regard to information security by directing and controlling organizations with coordinated activities. They should be committed to information security and should be able to contribute to the security objectives and protection needs of assets of the organization. They should have knowledge how to take information security into account in their managerial responsibilities. It is top management’s responsibility to get all personnel motivated to follow organization’s information security policy. Essential role of the top management is strategic management that is primarily related to change management for developing the whole organization to the future’s needs and expectations. In this context information security is strongly related to managing business risks, continuity, and crises.

As a rule, information security management is often only seen from the viewpoint of large corporations. However, even giant corporations are not islands, they are connected with other, smaller companies through subcontracting and outsourcing. As a result, negligence in the management of information security, may affect through the network. Commitment to information security is of utmost importance within the entire network. By their commitment, corporate managers help pave the way towards the information society (Savola et al., 2005).

2.3 New Challenges for Information Security and Related Experts and Professionals

At the expert level information security, knowledge is not only needed by the information security management professionals but also e.g. by R&D engineers who are developing ICT solutions and their security practices.

2.3.1 Developers of ICT Solutions

The developers of ICT solutions are an important expert group of the information society and business. The developers are involved with information security issues all the way from the beginning of system design cycle in a multifaceted way. Solutions development tasks are not only technical issues but information security designers should also take into account users’ behavioral aspects. In order to make information security solutions widely used in society the usability is an important design goal for security solutions. Irvine in “Challenges in Computer Security Education” (Irvine, 1997) identifies different expert groups and their needs:
• Software and hardware developers,
• System architects,
• System certifiers,
• CERT members, and
• Security researchers.

Development of security solutions is not carried out solely by security experts. Instead, engineers and other developers from different application areas should know how to take information security into account in an adequate way in their own area of specialization. Information security is strongly a horizontal competence area and security solutions are often different in different application fields. In general, there cannot be a security expert for every project case.

Challenges for good information security in designs are especially short project schedules in product development, increasing complexity and decreasing life of technical systems, and markets needs for short-term cost effectiveness. These challenges can be overcome only if understanding of information security becomes an intrinsic part, a “thinking model” of product and business development by using ICT solutions. How can this new thinking model be developed then? Certainly there is no fire-proof solution. However, key issue is the developers themselves having enough knowledge and skills related to information security and ability to work innovatively and collaboratively.

Understanding different phenomena and their dependencies is a big challenge for the research and development in the field. E.g. the research community has been long time guilty in investigating information security “through” certain vertical application areas but the horizontality and needs for multi-technology solutions has not been understood well enough. For example, in telecommunications, a lot of work has been devoted only to security end-to-end communication, encryption and authentication, forgetting what happens to the information outside of the communication link. The communicated information can be handled in different kinds of information systems, platforms and there may be many users of the information. A big challenge is to manage information security in complex and networked multi-organization cooperation. Innovation skills are required also in the research and development of information security.

2.3.2 Information Security Professionals

Information security professionals, such as CISOs (Chief Information Security Officers) are core people for developing information security approaches and tools in organizations and businesses. These professionals should have a multifaceted background and education in e.g. telecommunications, networks, risk analysis, contingency planning, and business management.
The principal role of an information security expert in an organization is to develop continuously the whole organization’s business capabilities to professional and excellent information security. Therefore metacognitive skills are especially significant for all organizational experts including information security specialists (Mayer, 1998). They should have ability also for making critically their own ideas questionable. An effective information security manager should have abilities for learning to learn. This person knows the stages in the process of learning and understands his/her own preferred approaches to it and can identify and overcome blocks to learning and can bring learning from off-the-job learning to on-the-job situations.

As the business situations and environments in general, also information security cases have become more complex. That means that also among information security expertise there are already many specialized sub-areas of expertise that may require specialized mathematical, technical, psychological, legal, organizational, cultural, etc. knowledge. One expert cannot be any more expert in the whole area of information security. The consequence is that experts should have active expert networks inside and outside organizations, and therefore networking and collaborative skills are essential. We have moved from individual knowledge to networked knowledge where the degree of connectivity, degree of interactivity, and degree of sharing knowledge between different experts is more important that what individual experts know.

Information experts should have deep knowledge of the general standards of the field. That includes especially the following recognized reference material:


General principles are a good foundation for information security experts to information security knowledge. For that OECD has produced recognized guidelines towards a culture of security (OECD, 2002). Those guidelines focus on the security of information systems and networks.

Information security experts should be well aware of the general standards for information systems. There are both international consensus standards and de facto standards. The following are the most important:

- ITIL, IT Infrastructure Library, 2006
- COBIT, Control Objectives for Information Technology (IT Governance)
- COSO Internal Control Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- The Sarbanes-Oxley Act, 2002
Also general business management models and standards, e.g. ISO 9000 standards, must be aware by information security experts. The use of all these reference materials is not at all an easy issue. Those documents are very comprehensive, overlapping and proposing different possibilities to approach. Information security experts must be able to select elements and the approach that are most suitable for his/her case.

In organizations information security is always contextual issue. Therefore information security expert should understand his/her organization’s business system and dynamics of business processes within the system. Especially it is important to recognize linkages of information security with business processes. One should be clearly aware of the interactive relations among organizational groups and have abilities to create and distribute new knowledge horizontally and vertically in organization by using normal business interactions. A challenge is to get effective communication happen between business leaders and information security experts.

Development of organizational information security solutions essentially aims at enhancing organizations’ business performance. Therefore, information security experts should have skills of change management. New general information security principles and recommendations are created by different expert communities of the information security. That means that information security experts of different organizations should be actively and continuously involved with international cooperation, e.g. standardization and preparation of national and international directions and guidance for information security. Major information society decisions are made by politicians. In order to take here into account also information security issues in a professional way, information security experts should be active also in cooperating with related authorities and in contributing for the development of society with their expert knowledge.

3 Traditional Training and Education in Information Security

In the following, we discuss how traditional training has been arranged at different levels of needs for information security education.

3.1 Enhancing Information Security Awareness among Citizens

Information security awareness among the large population of citizens has been increased by different means including:

- Comprehensive education
- General adult education
- Promoting information security by ICT system and service providers and institutional organizations or official bodies
- Articles in newspapers and magazines and television programs
- National campaigns

__________________________________________
www.security-conference.org
For promoting security culture, for example, Finnish Communications Regulatory Authority is carrying out a work in the National Information Security Day program, targeted for schools and SMEs. Today’s efforts in information security awareness enhancement represent a good starting point. However, a lot needs to be done to prepare for a ubiquitous digital society. The problem in current security awareness programs and education is that they typically offer only check lists for information security practices. Instead of check lists, more profound knowledge and holistic understanding of information security phenomena is needed.

In addition, there are Web services available for increasing information security awareness. These are especially to the young generation of Internet users. We have examples at European level (Tietoturvakoulu, 2007) and national level in Finland (Insafe, 2007).

It is important that information security becomes a fixed part of the education programs in comprehensive schools and vocational institutes. Nowadays, this education is not an integral part of any major subject in school. Comprehensive information security education relies on the activity of a few vigilant teachers.

Technical and economical vocational education is facing a big challenge of implementing information security education. They should be able to develop a holistic information security education program, with parts of information security management, technical solutions, legislation and business management. Focusing to teaching technical security solutions is not enough. Neither is enough to teach technical solutions only from the point of view of one vertical technology area, such as telecommunications, software or information systems. In addition, solutions are done at different levels of abstraction: system, module and more detailed levels. Sole concentration to information security management is neither enough. Information security management skills without technical understanding of solutions do not make good security experts. Current technical and economical vocational education is touching only the surface of information security. The result is that students are able to use and draft partial security check-lists, but are not able to see the whole picture of information security management.

3.2 Management Training and Education

Management training and education programs, e.g. MBA programs, do not normally include remarkably elements for managing information security. There are, however, available quite a lot of different seminars and consulting services for information security. In organizations and businesses there have been a lot of different information security training approaches and awareness programs and even e-learning means have been developed. (Walsh, 1996) (Thomson, von Solms, 1997) (Épelboin, 2002) (Kajava et al, 2003) (Kajava, Varonen, 2004) (Heikkinen, Ramet, 2004) (Neal et al, 2004) (Kajava et al, 2006-1)

Several studies made in different organizations indicate that often members of the management teams as well as key personnel in organizations are well-versed in
information security and its attendant risks. Yet, although they are even motivated to deepen their knowledge and hone their skills, it is not sure, whether they have internalized their own roles of management in information security. Top managers often have only a superficial understanding of information security management in practice, which may lead them to make decisions that are not conducive to raising the organization's information security performance. (Kajava et al, 2006-2)

In Finland the Ministry of Finance has appointed the Government Information Security Management Board (VAHTI, 2006) as a body for the co-operation, steering and development of government information security. The aim is, by developing information security, to improve the reliability and continuity of state administrative functions as well as enhance the integration of information security as an integral part of all state administration. The VAHTI guidance publications are widely utilized also in municipal administration, the private sector, citizen activities and international co-operation. As a consequence VAHTI publications are a significant vehicle in disseminating information security knowledge.

In Northern Finland we have created an information security network that has also contacts to key personalities globally. For communication and cooperation we are using modern blog technology (Information Security Network in Northern Finland, 2006). That is a place to distribute information and ideas on information security issues free for those who need it. The main idea is to promote work together by a networked manner.

3.3 Higher Level Education for Experts

Information security experts, e.g. CISOs, have typically acquired their knowledge by having a long working history in technical or administrative tasks. Most information security managers in organizations have university level education.

Nowadays many universities and technical institutes have had their own information and public security education B.Sc., M.Sc. and doctoral programs already since early 1990’s. If their own resources are not enough to arrange information security education in a proper way, co-operation between different schools and departments is taken place. We are still in the beginning of arranging the information security education, and networking in this challenging area is necessary. With a limited information security program we cannot produce real information security experts or business experts for the needs of industry.


In Finland information security education was stated at Oulu University in 1990. In 1997 there was some discussions with 20 delegated of European universities, which were interested about security education by participating Erasmus/Socrates projects. One topic
of discussions was how many Masters Thesis each university had per year. There were many who said – nothing. Some of the universities had one or two. From the perspective of Oulu university the situation was very special – there was six Masters in information security and it was not a good year for Oulu university. It is important to understand that university education in security is very new topic. On the other side, we must remember that the contents is still in many cases only technology / mathematics related. Those topics are still important, but besides those many other security topics are needed in university level education e.g. from legislation to ethical aspects of security. We particularly emphasize human and organizational points of security (Kajava and Varonen, 2000).

Now there are some changes coming in European universities for the quality of education? Well-known Bologna process (EU, 2000) is to harmonize education at all European higher level educational institutes. Danger is to create too bureaucratic solutions of quality assurance systems that are factually hindering genuine innovative development of quality in education.

For qualifying information security expertise, many professional certificates are nowadays used, e.g. CISSP (Certified Information Systems Security Professional), CISA (Certified Information Systems Auditor) and CISM (Certified Information Security Manager). Some certifications can be enhanced, e.g. CISSP-ISSEP (Information Systems Security Engineering Professional), CISSP-ISSAP (Information Systems Security Architecture Professional) and CISSP-ISSMP (Information Systems Security Management Professional). The purpose of certificates is to convince other people that the holder of a certificate is capable to carry out tasks in information security. The educative role of different certification programs can be in “fine tuning” or deepen the specific area of information security according to the role. Very often certifications seem to lack the connection to the basic studies of information security. Furthermore, more standardized certifications might be needed. It is not a goal that an expert has a long list of certifications in his/her business card.

4. Learning Knowledge of Information Security

In order to avoid the problems and miscarriage of the traditional training and education practices one should approach from separate training/education events or programs to continuous learning process integrated with the organizational business processes. It is necessary to have both individual and collective knowledge and learning in organizations (Senge et al, 1995).

Fundamentally learning means creating and cultivating mental models. Therefore a significant part of learning is reflection of learners own experiences. Information security knowledge is principally implicit (tacit) knowledge (Figure 1) and learning should be principally enhancing persons’ awareness in information security. Explicit knowledge, e.g. documentation related to policy documents, procedure documents, instructions, etc, is only a very minor part because most of the human activities are based is on tacit knowledge (Anttila 2004-1, Anttila 2004-2).
Integrated approach of information security strives for security related knowledge and activities that are linked with organization’s core competences and competitive advantages. In that way information security may become a strategic issue in an organization.

In learning approaches one should distinguish between single-loop and double-loop learning (Figure 2) (Smith, Argyris, 2001). In single-loop learning, individuals, groups or organizations modify their actions according to the difference between expected and obtained outcomes. That is typically operational level learning. In double-loop learning, the entities (individuals, groups or organization) question the values, assumptions and policies that led to the actions in the first place; if they are able to view and modify those, then second-order or double-loop learning has taken place. Because security experts’ principal duty in organizations is to develop continuously the whole organization’s information security performance professionally they should particularly focus on the double-loop learning. There are many types of learning by using different approaches and tools (see Table 1).

![Figure 1](image.png)

**Figure 1.** Most expertise knowledge is of tacit knowledge. Explicit knowledge has only a minor supporting role within practical operational situations (Anttila 2004-1).
5 Information Security Awareness

Integration of information security means that it is achieved naturally without any additional or artificial tricks, procedures, or systems in natural and real operational environments. This style of operating is fundamentally based on awareness within the responsible resources and organizations (Anttila 2006).

Table 1. Types of training and education (Siemens, 2006)

<table>
<thead>
<tr>
<th>Tool</th>
<th>For what?</th>
<th>Why?</th>
<th>Good for…</th>
<th>Drawbacks...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal learning</td>
<td>Courses, programs, degrees, defined by established knowledge, structure imposed by experts in advance of learning</td>
<td>Structure, serve stakeholders, focused</td>
<td>Initiating learners who are new (foundation building)</td>
<td>When learning at the point of need is required</td>
</tr>
<tr>
<td>Experience / game</td>
<td>Problem-based learning, ill-defined learning targets, user defined process and space, adaptive, flexible</td>
<td>Experiential (learning as a by-product of other activities)</td>
<td>Life challenges</td>
<td>If foundations are not in place (or the learning experience – as games – needs to provide foundation)</td>
</tr>
<tr>
<td>Mentor</td>
<td>Personal, guided and</td>
<td>Accelerate</td>
<td>Personal, Foundation</td>
<td></td>
</tr>
</tbody>
</table>
Information security awareness (or its synonym information security consciousness) is most essential topic for realizing information security and applying it in practical cases. The concept may be defined very simply: “having knowledge of information security”. However, what is the meaning of this is not at all any simple thing. Awareness is a profound totality of physical, psychological, and philosophical aspects of sensations, perceptions, ideas, attitudes, and feelings related to an individual or a group having knowledge of the abstract and comprehensive object of information security of a certain case, at any given time, or within a given time span. Different deepness-levels (Figure 3) of intellectual behavior in awareness and learning that may be categorized e.g. according to classical Bloom's Taxonomy (Lamb, Johnson, 2003). Meta-cognitive readiness and ability to learn learning and to open to question one's own way to think and act are the most sublime achievements in the development of learning (Mayer, 1998).

<table>
<thead>
<tr>
<th></th>
<th>facilitated by expert personal performance relevant knowledge/learning forming, high bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance support</strong></td>
<td>Learning at the point of need can rely on other learning approaches Point of need, competence, assistive Short focused learning Developing foundations of a discipline</td>
</tr>
<tr>
<td><strong>Self-learning</strong></td>
<td>Meta-cognition, learning about learning, Learning that is personally driven Learning for pleasure, personal competence Exploring areas of personal interest How do learners know what they need to know?</td>
</tr>
<tr>
<td><strong>Community-based learning</strong></td>
<td>Diversity, “Wisdom of the crowds”, social/dialogue Create multi-faceted view of a space or discipline Dialogue, diversity of perspective Foundational high time requirement</td>
</tr>
<tr>
<td><strong>Informal learning</strong></td>
<td>Conferences, workshops, colleagues Serendipity, constant, ongoing, in the stream Continual, ongoing, multifaceted Chaotic, not always valued, scattered</td>
</tr>
</tbody>
</table>
1. Know  
Passive knowing, reproducing, and quoting knowledge produced by others

2. Comprehend  
Finding meanings, interpreting facts, inferring cause & consequence

3. Apply  
Active applying knowledge in new situations, solving problems

4. Analyze  
Recognizing and explaining patterns and meanings, seeing parts and wholes

5. Synthesize  
Composing knowledge, creating new ideas, predicting and drawing conclusions

6. Evaluate  
Assessing value and making choices and recommendations for innovative reforming, critiquing attitudes and beliefs

6+. Metacognitive skills to understand how the learner learns. Awareness of one's own knowledge and ability to understand, control, manipulate, and making own ideas questionable

**Figure 3. Different depthness-levels of intellectual behavior in awareness and learning**

Very often today through traditional formal information security training and education one can achieve only very first levels of the Figure 3. However, in order to ensure development and maintenance of information security in organizations and in societies at large in ever changing operational environments and with fast development of ICT technology, we should have even deepest level of awareness among our information security experts within our organizations. All actor categories need deep knowledge but contents required are different in different categories. Even citizens need that kind of knowledge because they may meet unexpected situations during their everyday activities.

Awareness-related phenomena are essential but also very complex things when developing information security approaches in any kind of organization in modern business environments. There are always also complex connections between consciousness and unconsciousness (sub-consciousness). Situation is still more complicated when one is considering possibilities of the collective consciousness and collective unconsciousness. (Block, 1995)

Consciousness is difficult to define or locate, and it involves a lot of disagreements depending on one's philosophical paradigm. Some have even argued that empirical tests of consciousness are intrinsically impossible.

In biological psychology awareness implies somebody's perception via physiological senses and reaction through mental information processes to a condition or event. This type of awareness does not necessarily imply profound understanding. Awareness is a relative concept. One may be partially aware, may be subconsciously (unconsciously) aware or may be acutely aware of an event. Awareness may be focused on an internal state or on external events by way of sensory perception. Awareness provides the raw material from which one develops subjective ideas about his/her experience. Phenomenal consciousness consists of mental events of experience, including forms with different
qualities, sensations, emotions and feelings with us and our responses. In access consciousness a mind is directed at something. Information security is always a perception of someone who has something to do with the entity in question. It is quite obvious that a lot of information security risks are originated from problematic situations in someone’s mental process.

Events that occur in the mind or brain that are not within phenomenal consciousness are unconscious events. We have always complex and unidentified transactions between one's consciousness and unconsciousness. Carl Jung introduced the concept collective unconscious (Boeree, 2006). That related essentially to his idea of archetype. The archetype implies common psychological predispositions of humans. Archetypes can only be revealed through an examination of the symbolic communications of the human psyche, and the themes of human relational/behavioral patterns. Archetype is defined as the original model of which all other similar objects or concepts are merely derivative, copied, patterned, or emulated. Social networking, communication and imitation of memes are the major processes related to sharing in the archetypes. In the case of information security it is essential to understand what those basic archetypes of information security are really. Obviously appreciating one’s privacy is in the core of information security archetypes. After understanding archetypes of information security one may approach to the guiding principles for managing information security in practical cases. However, this archetype approach is not familiar even among the real experts.

5 Modern Learning Theories and Facilities Enhancing Information Security Awareness

Successful operations in information society and management of organizations are based on right knowledge and skills to use the knowledge for the current needs. Additionally, exchange of information is necessary between organizations’ customers, employees, shareholders, suppliers, business partners, and the great public.

Organizational and personal learning are prerequisites for enhancing information security skills in striving for successful operations in information society. On-the-job learning offers cost-effective way to link learning to the organizational needs and priorities.

The aim of the new approach in learning is to improve learning through improving interactive communication, and building social knowledge within organizations and communities. In this approach, management learning is integrated with normal managing activities of the business leaders. That means that learning takes place while in actual performance of business leaders’ work.

There have been a lot of positive expectations and promises for e-learning solutions especially based on standardized approaches like SCORM, AICC, and SingCore ADL (2004) (AICC, 2006) (Marshall, 2004) (Siemens, 2004). Practical experiences, however, prove that these approaches do not provide solutions for effective on-the-job learning. Only basic information security skills may be learned by traditional training programs.
Business people are busy and not genuinely interested in using ordinary e-learning means. In the first stage of e-learning it was understood only as usage of new technological solutions facilitating distant learning and automation of certain training activities. The next stage was the development of particular “learning management systems” in order to manage training activities comprehensively. Here we confront the same problems as in the quality system approaches in the European universities (EU, 2000). Still traditional training theories and practices are followed in learning management systems, e.g. training is still based on course structures. Experiences at least in business environments have not been encouraging. The learning systems are too expensive and stereotyped, the learning too boring, the search of material (learning objects) too cumbersome, the reusable objects not really reusable. One should note that also the decay time of knowledge – and especially needed by business management and ICT governance – has been remarkably shortened.

Behaviorism and objectivism, cognitivism and pragmatism, and constructivism and interpretivism have been the most significant learning theories and traditions utilized until now in the training and education. Learning needs and theories that describe learning principles and processes should be reflective of today’s underlying social environments. Quality in e-learning requires application of new learning theory-approaches like connectivity, interactivity, and sharing information (Gloor, 2004). New social software technology gives possibilities to realize these new learning theories in practical cases particularly in business organizational environments. It also facilitated learning in networks which is now practical situation in all business cases. (Siemens, 2006) (Siemens, 2004) (Downes, 2004)

Today learning objects are not presented ordered, in a sequence, but randomly, unordered. That does not take place in classrooms or schools but in the living/working environment, where people find themselves. We don’t present them at all, we contribute them to the conversation, and we become part of the conversation. They are not just text and tests; they are our publications and speeches, our thoughts in real-time conversation and communication.

Leadership and expertise emphasize personal and human aspects in carrying out business resources and actions, and are based on persons’ inherent understanding, knowledge and behaviours. A great challenge is to combine explicit and tacit knowledge in all management and expert decisions, and to get knowledge moved from individuals within the whole organization between different actors, and from tacit domain to explicit domain and also vice versa. Working collaboratively by using intellectual capacity of the whole organization is the target for business benefits. A well-known foundation for knowledge transformation has been created by Dr. Nonaka and his Japanese co-researchers. They defined the SECI process for knowledge transformation from tacit to explicit and vice versa: Socialization - Externalization - Combination - Internalization of the knowledge (Nonaka et al, 2000).

Modern learning environments are to facilitate effective and efficient knowledge-intensive and networked learning activities. These environments provide means for learning through improving interactive and collaborative communication of management,
and building social knowledge and intelligence. Learning is integrated with people’s normal activities.

The new facilities are to realize new learning theories in practical cases in educational institutes and organizations. They facilitate learning in networks which is situation in all practical cases. Knowledge-intensive networked learning facilities (Anttila, 2006) consist of ability to lead learners into electronic work areas (Figure 4), where they operate in collaboration to learn by building new knowledge. They have also all relevant explicit information easily available through related documents. The basic tools include blog, wiki, aggregator, forums, and files that are based on modern proved social software or Web 2.0 technology (O’Reilly, 2005). Software for the tools-components is typically created by the open source software community that is the biggest resource in the world for developing software products. Software is inexpensive compared with large e-learning systems, or they are available free of charge. Open software is easy to modify and customize, and it provides rapid application development. (Arina, 2006)

The method of reflecting on experience (blogs) and building knowledge models (wiki) collectively produces results that can be blogged further to other teams or individuals. This creates a digital pipeline or an intelligent link for knowledge building. Technology of these tools and popularity of their benefits have been proved in large scale public use in Internet. Now a big challenge is to use those tools also internally in organizational business purposes and especially in the business management process. Within collaborative learning environments, learning evaluation can be also carried out by using new interactive evaluation methodologies (ZEF, 2006).

Information security expertise is a very suitable example of specialized learning where this new learning approach can be used. It is strongly knowledge-based collaborative and innovative activity, and typically involved in organizations by board of directors, executing managers, selected experts, personnel and stakeholders’ representatives. Especially benefits of using this approach are obvious in cases where participants are geographically scattered and where arranging synchronous of physical meetings is difficult.
Figure 4. An example of a practical user interface to the knowledge-intensive collaborative on-the-job learning environment for information security

6 Conclusions

It is impractical to require that everybody needs to know everything about information security. Knowledge and skills appropriate to each role in the information society must be identified. The needs can be classified to three levels: basic information security literacy level, advanced level and expert level. Users of information systems – all members of society – should be at least basic information security literate. In the day-to-day business life, advanced skills of information security management are needed. At the expert level, the developers of technical and administrative solutions need to have a wide understanding of information security threats and solutions. It is essential that the education world can answer the needs of different actors in society.

Many professional certificates are nowadays used in information security. They have been used to convince other people that the holder of a certificate is capable to carry out tasks in information security. However the certification programs ensure only very basic knowledge that may even be rather superficial and stereotyped.

Traditional training and education approaches are not enough for information security in the modern knowledge-intensive businesses and societies. New learning theories and new practical Web 2.0 applications have proves effective and useful in learning based on increasing degree on connectivity, degree of interactivity, and degree of sharing information between experts, business leaders, and ordinary citizens.
References

Kajava J, Savola R, Varonen R and Anttila J. (2006-1). Exploring the use of an e-learning environment to enhance information security awareness in a small company, the CIS2006 conference, Guangzhou
Heikkinen, I., Ramet, T (2004). E-Learning as a part of information security education development from organizational point of view, Oulu University, Oulu (in Finnish).
Nonaka, I; Toyama,R; Konno, N (2000). SECI, Ba, and leadership: A unified model of dynamic knowledge creation, Long range planning 33, Pergamon