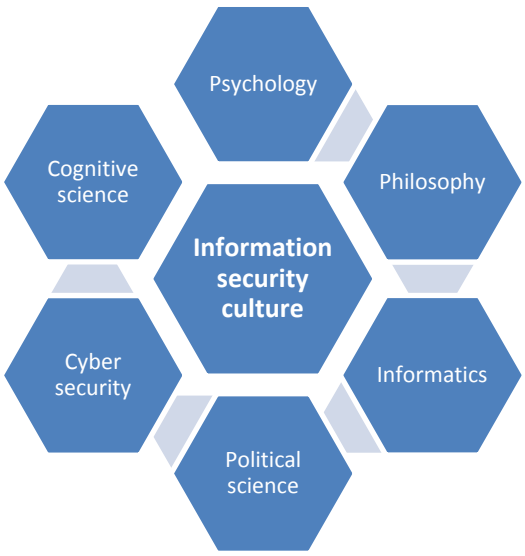
SECURIT

Security Culture and Information Technology

The research program Security Culture and Information Technology, SECURIT, aims at improving the information security of organizations. In contemporary information-intensive organizations, a good security culture is vital for the information security.

The research is jointly performed by Chalmers University of Technology, FOI, the Royal Institute of Technology, the University of Gothenburg, and Örebro University in cooperation with Linköping University. Karlstad University coordinates and supports the Swedish IT Security Network for PhD students (SWITS) with funding from SECURIT.

The researchers come from various subject areas, as illustrated in the figure below. Thus, the program will provide multi-disciplinary views on issues related to information security culture.



SECURIT includes nine research projects addressing different aspects of information security culture. The results are continuously disseminated through scientific publication and other forms of presentation.

Contact: Jonas Hallberg, jonas.hallberg@foi.se

SECURIT is funded by the Swedish Civil Contingencies Agency (MSB) and coordinated by the Swedish Defence Research Agency (FOI).

The program was launched in July 2012 and is planned to continue through September 2017.

What is information security culture?

The researchers participating in SECURIT have agreed on the following definition of information security culture.

Shared patterns of thought, behaviour, and values that arise and evolve within a social group, based on communicative processes influenced by internal and external requirements, are conveyed to new members and have implications on information security.

The process resulting in this definition is presented in the document *Definition of information security culture* (FOI Memo 5253).

Research projects

The main research efforts carried out within the SECURIT are performed in the nine research projects included in the program. In the below figure, the scheduling of the projects is illustrated. Overviews of the projects are provided in the following subsections.

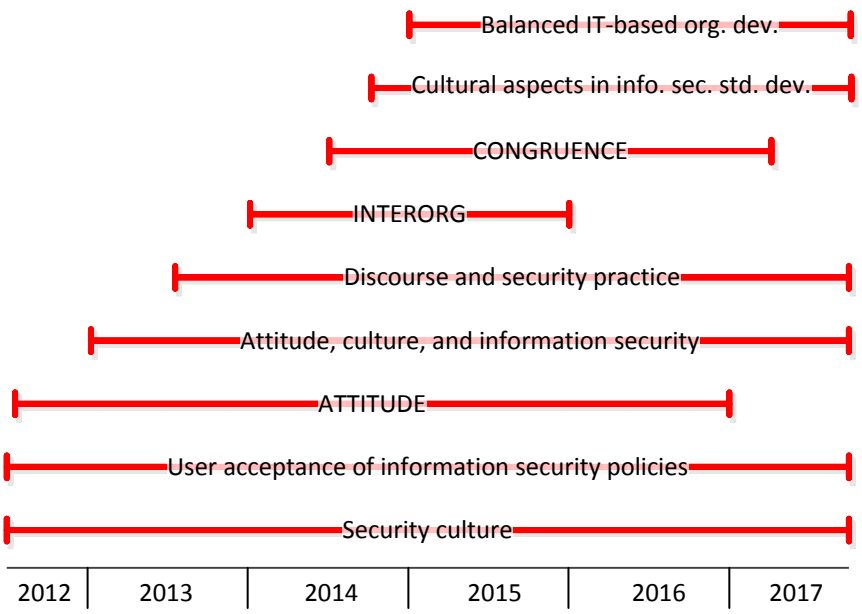


Figure 1: The scheduling of the research projects included in the SECURIT program.

Security culture

Project manager: Sven Ove Hansson, Royal Institute of Technology

Duration: July 2012 to September 2017

Although safety/security culture has been studied to a considerable degree, relatively little is known about how the security culture relates to the general social and intellectual climate in organizations. A necessity is to define information security culture and related concepts. Thereafter, the relations between the defined concepts can be studied. For example, this may include the relations between efficiency aspects and the various aspects of security culture.

The main goal of this project is to capture the relation between security culture and the general culture or climate in an organization, and in particular the relation to cultures such as the efficiency and privacy cultures. The work will further the understanding of information security culture, related concepts and their relations and support the improvement of the security cultures of organizations.

User acceptance of information security policies

Project manager: Jonas Hallberg, FOI

Duration: July 2012 to September 2017

In contemporary information-driven organizations most employees take actions that influence the information security. Thus, their behavior becomes a factor in the equation deciding the information security of organizations. A common practice, which is intended to lower the information security risk, is to establish an information security policy. Information security policies describe, for instance, the consequences of security policy violation, the acceptable use of computer resources, the responsibilities regarding information security, and the type of training that employees should have.

This project focuses on behaviour related to the information security polices and factors that influence their acceptance and utility. Among the factors investigated, the information security culture and climate of organizations are included. Three themes are to be investigated during the project:

1) Factors influencing the compliance with information security policies and similar security-related behaviour within organizations.
2) The risk perceptions of individuals and groups and the relationship between information security risk appetite, policies, and compliance.
3) Information security incident management and its effect on the information security of organizations.

The results of the project will help information security managers understand the way the studied factors influence the information security of their organizations and, possibly, to influence the security culture of organizations in a controlled manner in order to govern employees information security behaviour. The knowledge developed within this project will make it possible to develop tools and guides that support information security management.

Attitude, culture, and information security

Project manager: Anders Pousette, University of Gothenburg

Duration: January 2013 to September 2017

The project is focused on information security (IS) within the healthcare sector. Healthcare is a highly complex operation that involves processing of sensitive information about patients. The quality of care is dependent on the availability of accurate and timely information. In the health care sector, information security is thus a critical issue for quality of care and patient safety. But the properties of the sector also make it highly suitable for the study of IS phenomena that may be generalized to other industries.

Two studies are carried out within the project; one using qualitative methodology (study 1) and one using quantitative methodology (study 2).

- The overall goal of study 1 is to describe the process of formation of a security culture in healthcare, and the rational grounds among healthcare practitioners that may explain the quality of the emerging culture.
- The overall goal of study 2 is to investigate the influence of information security climate on practice in day-to-day work.

The aim of the project is to investigate leadership and workforce attitudes to explain the formation of security cultures and climates within organizations, as well as the influence of security climate on IS in day-to-day work.

- How does the tension between the design of the information technology, the organizational demands of the work, professional cultures and the needs of the patients influence the formation and quality of an information security culture?
- How does the information safety climate (culture) affect the users' IS critical behaviour?
- How can we understand the variation in IS-climate in relation to the organizational context?

Discourse and security practice

Project manager: Peter Johansson, University of Gothenburg

Duration: July 2013 to September 2017

The Discourse and security practice project has two aims. The first aim is to investigate how discourses on human rights and democratic values inform and influence the development of information security systems where large quantities of sensitive data on citizens and patients are collected and stored. This aim is fulfilled through two subprojects.

- The first subproject (study 1) focuses on articulated discourses concerning the new biobank law under development in Sweden.
- The second subproject (study 2) focuses on the new personal web-based health account HälsaFörMig under development by eHälsomyndigheten by order of the Ministry of Health and Social Affairs. HälsaFörMig will serve as a hub for the subproject in terms of identifying relevant discourses articulated in the eHealth sector in Sweden.

The goals related to this aim are

- to inform how concepts and norms linked to the human rights discourse (such as individual privacy) are interacting and competing with public and private interests in the development of information systems collecting and storing large quantities of sensitive data on citizens and patients
- to problematize assumptions about the individual/patient as a rational, autonomous and socially independent actor who can make appropriate decisions in a context characterized by uncertainties about the cumulative effects on privacy and information security

The second aim of the project is to investigate attitudes to whistleblowing and freedom of information and how these values affect behavior and attitudes relating to information security systems. This aim is fulfilled through a survey (study 3) focusing on questions regarding freedom of information and whistleblowing.

The goals related to this aim are

- to measure attitudes towards whistleblowing and freedom of information

- to analyze the link between attitudes towards whistleblowing and freedom of information and attitudes towards information security regulations
- to analyze the link between attitudes towards whistleblowing and freedom of information and information security behavior

The project will inform MSB to what extent privacy and other fundamental human rights inform and influence the development of large information security systems today and what is lacking in those regards. The three case studies will provide in-depth knowledge about the ways in which issues of privacy and integrity are present or absent in discussions about, and design of, information security systems and policies. On a general level, the result of this study can be used to identify the need for further research in this area, but also to develop best practices and/or guidelines for how to safeguard a balance between democratic values and information security systems in the future. The results of the study may also be used to develop information security work within organizations, for instance by pointing to the need for holistic approaches to information security, where technical and security requirements need to be weighed against other values such as fundamental rights and social impact.

Balanced IT-based organizational development

Project manager: Jonas Landgren, University of Gothenburg and Chalmers University of Technology

Duration: January 2015 to September 2017

Emergency call actors handle on an everyday basis, records of sensitive personal information that cannot easily be shared between the parties involved. Further, these actors undergo continuous technological-based organizational development.

The project will use findings from the two projects Attitude, culture, and information security and Discourse and security practice as important input, and further advance the results by exploring how these challenges are addressed in safety and security dependent organizational environments.

The aim of the project is to investigate how IT-based organizational development could be shaped to improve design, implementation and use of information systems, integrating and balancing the high demands on security, usability, integrity and human rights. The project is focused on how to address the challenges of providing a viable balance between high-level of security, strong usability and accommodation and protection of personal integrity and human rights.

ATTITUDE

Project manager: Joachim Åström, Örebro University

Duration: August 2012 to December 2016

Contemporary studies on information security culture often take the organization as a rational instrument designed by top management to shape the behavior of employees in purposeful ways. The study of information security culture typically takes culture as the independent variable, without attempting to understand why patterns of attitudes and values may vary across contexts. In addition,

it is conceptually possible to make a distinction between organizational culture and information security culture, but the question is if it is possible and fruitful to do so in empirical studies. We will therefore study the importance of organizational culture to employees' information security attitudes and behaviors. In addition, we have identified methodological issues related to information security compliance measures in quantitative studies, which to a limited degree seem to acknowledge the importance of value pluralism; instead most existing measures are based on a value-monistic view on organizations and management.

A value pluralistic view means that employees should not or cannot simply serve as the instruments of the particular values that are promoted by one category of managers, such as information security managers. Put another way, one group cannot monopolize the management discourse in an organization. Instead employees need be able to follow multiple organizational imperatives that are anchored in different, sometimes conflicting, value systems in the organization. Consequently, the project will also study methodological issues related to measuring employees' information security attitudes and behavior.

The project will investigate the link between organisational culture and information security attitudes and behaviours. More in detail we intend to focus on the effects of different types of organisational cultures on employees' information security attitudes and behaviours. Second, the project will also contribute to the debate on how to measure employees' information security attitudes and behaviours.

The study increases the awareness of how different types of organisational culture affect employees' information security attitudes and compliance behaviours. It provides a baseline for current information security attitudes and compliance behaviours in Sweden, and where the largest challenges are found in relation to organisational culture. In addition, the contribution made to methodological issues on how to measure employees' information security attitudes and behaviours can be important in future survey measures for practitioners (and researchers).

On the overall research program-level cultural aspects are measured in several ways since several projects in the SECURIT-program collaborate: as organisational culture and as information security climate and as individual information security attitudes.

INTERORG

Project manager: Frans Prenkert, Örebro University

Duration: January 2014 to December 2015

Every organization has a particular culture, comprising a ubiquitous set of assumptions that is often difficult to visualise, and that directs the activities within the organisation. A rather simple definition of culture is; the beliefs and values shared by people in an organisation. But oversimplifying the concept may also be the biggest danger to understanding it and the same scholar who provided the definition has also given a more elaborated definition to show the complexity at hand: "The pattern

of shared basic assumptions- invented, discovered or developed by a given group (…) that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel" (Schein, 1999)[1]. Irrespective of a simple or complex definition, existing research (e.g. Hedström et al. 2011)[2] on information security has shown that goals, beliefs and values, affect how information security actions as well as other actions are carried out in organisations.

As beliefs, goals and values govern peoples' actions, they also govern the design of information security policies and the choice of technical information security. Together these parts make up the information systems (people, processes and information technology) in an organization. The information systems can put emphasis on the different parts of information security, for example on different parts of the confidentiality, integrity and availability (CIA-triad), or on the complementing RITE-principles (responsibility, integrity (role integrity), trust, ethics) presented by Dhillon. Since collaboration between organisations is becoming more and more important in today's society it is of interest to see how different sets of beliefs, goals and values (in other words culture) directs joint activities between organisations. Our literature review (part of the Interorg-project) has shown that such studies are missing in existing research.

The aim of the INTERORG project is to develop knowledge of the character of conflicts between information security cultures in inter-organizational contexts.

The results from this study increase awareness of how information security culture affects collaboration in inter-organizational settings. Such awareness is important and can help information security managers in their work with cultivating information security cultures in organizations. Furthermore, we also create a more nuanced understanding of how information security culture in an organisation evolves, and that it is not isolated from what happens in other organisations.

CONGRUENCE

Project manager: Fredrik Karlsson, Örebro University

Duration: July 2014 to March 2017

Organizations are often required to implement different standards for information security, for example ISO-27000. There are currently many different tools used to ensure that the standards are implemented and that they are working effectively as intended. Examples of such tools are training documentation, policies, regulations and guidelines used. To maximize the effects of change, it is important that these tools are in harmony. Otherwise, the different tools might communicate different rationales. Thus, this project will contribute with knowledge about how to construct tools

[1] Schein, Edgar. (1999). *The Corporate Culture Survival Guide: Sense and Nonsense about Cultural Change*. San Francisco: Jossey-Bass.

[2] Hedström K, Kolkowska E, Karlsson F, Allen JP (2011) *Value conflicts for information security management*. Journal of Strategic Information Systems, Volume 20, Issue 4, 373-384

from a multi-actor perspective that communicate congruent information systems (IS) goals and values.

The final deliverables will support:

1) identification of challenges, and
2) guidelines for how to govern congruent information security and related artefacts.

The aim of the CONGRUENCE project is to develop knowledge on how to ensure that the governance tools used to transform the information security culture in an organization are in harmony, clearly and with certainty communicating the organization's information security culture.

MSB could use this knowledge to elaborate on guidelines for effective implementation of information security standards in organizations.

Cultural aspects in information security standard development

Project manager: Fredrik Karlsson, Örebro University

Duration: September 2014 to September 2017

Information security standards are best practices developed by information security experts globally. Hence, they indirectly influence how information security cultures develop in organizations since standards are often used as starting points for local information security work, such as in the implementation of information security management systems. For example, in Sweden it is required that public authorities implement ISO-27000. Currently, insufficient attention is devoted to how information security standards are co-constructed in processes creating meanings, trust and settling social structures. This project focuses on the co-construction of information security standards, such as the ISO 27000-series. We will uncover the culture behind information security standard making, investigate the shared pattern of values, mental models, and activities that are negotiated among standard making experts over time, affecting the "best practices" that are included in information security standards.

The project will

1) uncover the co-construction of information security standards, and

2) uncover the culture behind information security standard making.

Increased knowledge about information security standard making and how the culture behind information security standard making affects the so-called "best practices", which are pushed in these standards. MSB can use this knowledge to elaborate on advice and guidelines on information security standard making as well as information security standard use.