The Influence of the Human Factor on ICT Security: An Empirical Study within the Corporate Landscape in Austria

Christine Schuster
Institute for Empirical Social Studies
Vienna, Austria
e-mail: christine.schuster@ifes.at

Johannes Göllner, Christian Meurers,
Andreas Peer, Peter Prah
Section Knowledge Management
Department of Central Documentation & Information
National Defence Academy of the Austrian Federal
Ministry of Defence and Sports
Vienna, Austria
e-mail: {johannes.goellner | christian.meurers |
andreas.peer | peter.prah}@bmlvs.gv.at

Martin Latzenhofer, Stefan Schauer
Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
e-mail: {martin.latzenhofer | stefan.schauer}@ait.ac.at

Gerald Quirchmayr[1], Thomas Benesch[2]
[1]Research Group Multimedia Information Systems
Faculty of Computer Science
[2]Institute for International Development
University of Vienna
Vienna, Austria
e-mail: {gerald.quirchmayr | thomas.benesch}@univie.ac.at

***Abstract* — The human factor is a decisive risk factor in information security and is now on its way to be fully integrated into information security programs and risk management approaches. Due to this remaining lack of integration, we have designed a study on user attitudes towards information security issues in Austrian companies. This study included a comprehensive survey that was based on extensive desk research on risk, behavior and trust models. The second key part of the study reflects the results of two moderated focus groups that discussed information security issues derived from the analyzed literature. The third main component of our study is based on personal interviews with 891 respondents structured by the prepared survey. The analysis of the results from the focus groups and the personal interviews allowed the identification and confirmation of user perceptions and trustworthiness factors. Building upon the survey results, we propose a set of significant indicators that can help to identify ICT-related misuse and fraudulent behavior as a situation awareness instrument.**

Keywords— information security; user perceptions; attitude; human risk factor; work satisfaction; compliance.

I. INTRODUCTION

The trust employees have in their organization's information and communication technology (ICT) systems plays a crucial role when considering the organization's overall security situation. This has been emphasized by a comprehensive empirical study on ICT security in the corporate landscape in Austria carried out by the authors in 2015 and firstly presented at SECURWARE 2017 in [1], and is also amply discussed in the literature from various perspectives [2] [3]. Further, the attitude of employees as an indicator of emerging problems has also been described in recent publications [4] [5]. The key issue here is that the human behavior represents a major risk factor and is hard to control from an organization's perspective. Neither can these non-technical vulnerabilities be measured nor is there a real-time early warning system covering this aspect in a sufficiently reliable way. Repetitive awareness measures help to strengthen an organization's culture, but their effectiveness is hard to assess and those measures take a long time and many iterations. So far, there is no satisfying and reliable method that can be applied with reasonable effort to assess the human risk factor in an organization's environment [6] [7].

The afore mentioned empirical study was part of the project MetaRisk [8], which was supported and partially financed by the Austrian National Security Research Program KIRAS. The survey was conducted among employees with and without management functions. Based on the results of this survey, we investigated the situation regarding information security in Austrian companies in 2015. The key questions covered by this survey were the following:

1. How do individual staff members apply the safeguards that have been set up by their organization?
2. How do employees handle security-relevant incidents and, especially, which activities do they undertake to avoid or circumvent those incidents including activities that cause harm to the organization?
3. What is the general relationship between employer and employees?

By analyzing the employees' attitudes, tendency of activities and behavior patterns, we have identified possible indicators which can even point to insider fraud in extreme cases.

In the context of information security, the human aspects assume a decisive role as either an early warning of decaying information security awareness or as a careless attitude towards the issue. The continuously growing number of phishing, spear phishing and identity fraud attacks against

normal and unexperienced users shows that these types of attacks have recently become even more attractive [9]. With more sophisticated forms of attacks, for example advanced persistent threats (APT) where perimeter controls substantially lose their protective effectiveness [10], the problem becomes more critical. These forms of attacks are trying to obtain an organization's most confidential business information, causing financial damage and in stealing trade secrets. On the other hand, economic pressure is growing in general and both employees and employers are trying to reduce cost, aim for leaner processes and at minimizing efforts, thus making the work environment less comfortable. This is one reason why the potential for misuse, business and cybercrime is rising [2] [7]. A small but significant set of indicators reflects the attitude of the employee towards the information security situation in an individual organization. Consequently, if we look at this set of indicators all together we can identify the principal vulnerabilities of an organization related to the human risk factor. If we link these indicators to particular types of attacks, e.g., social engineering, we can decide whether an organization is more vulnerable than another.

The present paper is structured into five sections. In Section II, we first present the scientific basis from the relevant literature and our motivation for the study. Section III describes the applied methodological approach of the survey performed for the study. In Section IV, we discuss the main results of the study compared to retrospectively documented attack stories from real life. Section V proposes aspects for further research and we present concrete indicators that can serve as basis for forming a radar chart and as input for a scorecard. This leads to a general overview of the influence of human risk on information security.

II. Motivation and Background

As amply described in a large number of recent publications including textbooks, information security is an issue of continuously growing importance for organizations of all sizes. Recent trends in Austria [11, p. 8] [12] [13] and Germany [14] [15, p. 7] (the German situation is closely comparable to the Austrian one) have been a shift in attacks towards social engineering and fraud. An analysis of attack types performed in 2014 [16], shows which types of attacks were most successful in affected enterprises (Figure 1).

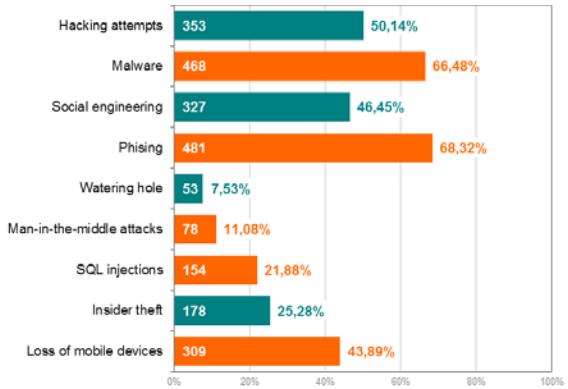

Figure 1. Successful attack types in affected respondent's enterprises in 2014, n=704 respondents [16, p. 6], edited

In this context, "phishing" attacks had the highest success rate, followed by the classic attack types "malware" and "hacking attempts" and by "social engineering". When looking at the latest, updated results of this study from 2015 [17], we can see that "social engineering" has surpassed the hacking attempts, now taking the third rank after "phishing" and "malware" in the list of the most successful attack types (Figure 2).

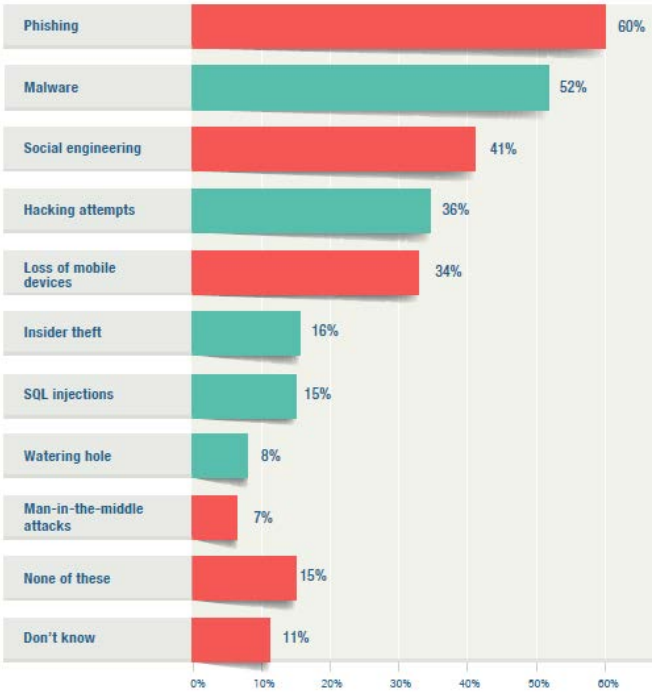

Figure 2. Successful attack types in affected respondent's enterprises in 2015, n=461 respondents [17]

The Austrian internet security report 2015 [12, p. 45] also explicitly states that social engineering methods are growing significantly in number and sophistication. This sort of attack can be seen as the currently most dangerous attack type. Therefore, the human factor has turned into the weakest link in the cyber defense chain of an organization.

As these attacks have a significant financial impact on affected companies [16], it is important to know the human vulnerabilities towards social engineering attacks and financial fraud that use information technology as a vehicle to commit crime. In one extreme case, such a financial fraud attack on an Austrian aerospace manufacturer recently caused an estimated damage of 50 million EUR [18]. Figure 3 illustrates this financial risk by pointing out that in 2014 almost half of US companies suffered financial damage from attacks at least annually [19, p. 28], while in 2016 the number of companies in the US which suffered damage of more than one million USD due to cybercrime doubled (i.e., from 7% in 2014 to 15% in 2016) [20]. At the same time, employees and managers are more and more ignorant of the impacts of cybercrime with just slightly more than half of the US companies having a cyber incident response plan that is "fully in operation" [20].

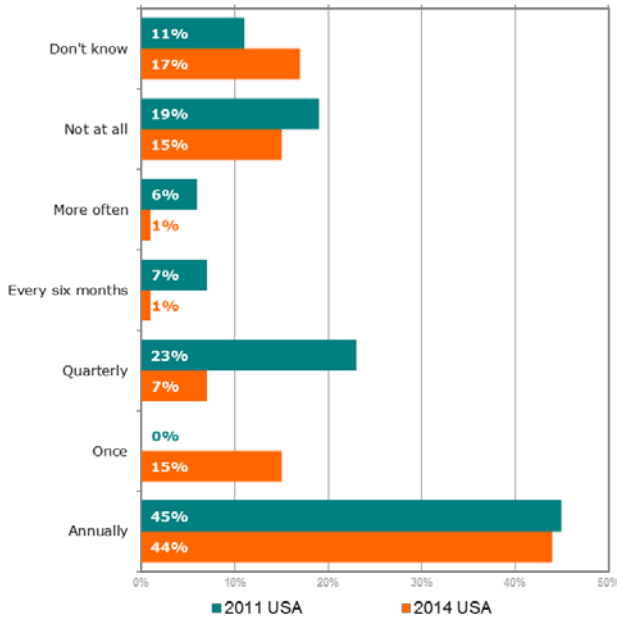

Figure 3. Relative financial impact
of cybercrime on organizations [19, p. 28], edited

Figure 4 clearly shows that insiders – no matter whether they have malicious or non-malicious intents – contributed significantly to the damage that enterprises suffered in 2014 [16].

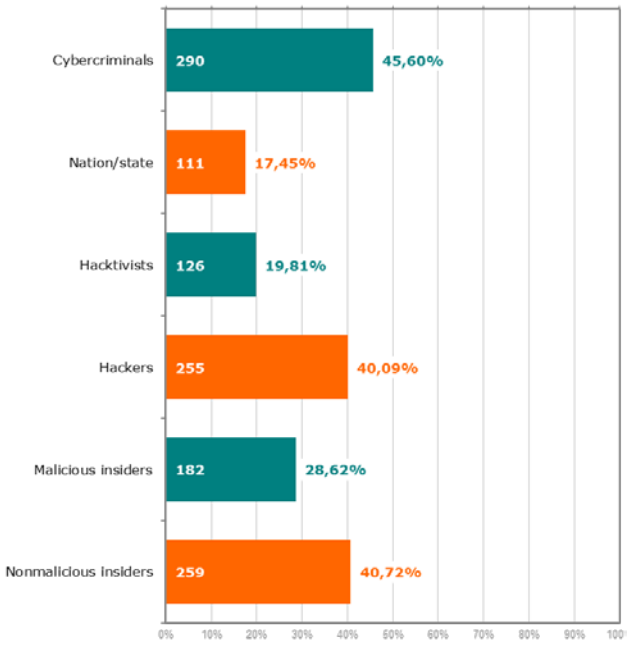

Figure 4. Threat actors 2014 [16, p. 5], edited

The risked posed by insiders has been confirmed in the 2015 report in [17] (Figure 5). This means that insiders will very likely continue to pose a high risk of security incidents also in the future.

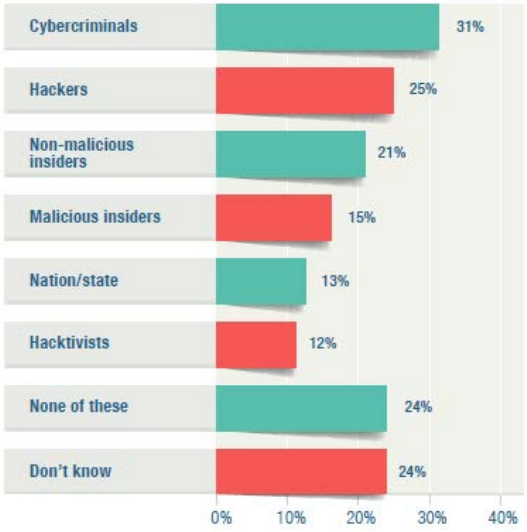

Figure 5. Threat actors 2015, n=461 respondents [16]

The list of threat actors consequently raises the question of how to ensure expected behavior of involved persons in an organization. The term compliance can be defined as the sum of all reasonable measures that address lawful and rule-consistent behavior of a company, its members and employees with regard to legal commands or prohibitions. The business integrity should also be consistent with social guidelines, moral concepts and ethical behavior [21]. In contrast, non-compliance entails all forms of non-observance of guidelines. It can be measured in terms of the seriousness of the infringement and can be categorized into violations that damage the company itself or employees. Three underlying motivational factors for divergent or non-ethical behavior of or within companies have been discussed in the literature: first, non-compliance can be justified by the personal benefit that employees gain by violating regulations. Second, the company as a whole can derive benefits from delinquent behavior. Third, non-compliance can be used to deliberately harm the company or external stakeholders [22, p. 225f]. Various factors might increase the likelihood of non-compliance: difficult working conditions; competitive pressures; unrealistic objectives and focus on simplistic success parameters; too much or too little control within a company's control system; management style; and corporate culture [22, p. 233ff].

In general, working conditions can be divided into three categories; macro, meso and micro level [23]. Raml [24, p. 87ff] allocates economic and social conditions, such as career perspective, economic situation, social status, balancing of family and working life to the macro and meso level. Similarly, work structures and resources (work organization, time models, work atmosphere, career opportunities, bonus payments, information related to work) belong to the macro and meso level [24]. On the other hand, resources and stress are located at the interface between employees and their own work, and are therefore assigned to the micro level [24]. This entails the scope of action, work contents, professional qualification, disturbances and

interruptions in daily routine, too many regulations and restrictive surrounding conditions.

It is widely accepted that insiders pose a special form of threat to businesses, institutions and organizations [25] [26] [27]. Insiders are persons who have a legitimate access to components of the ICT infrastructure. In contrast to external hackers, they have always at least one access point to ICT systems, and thus they do not require time consuming efforts to obtain additional privileges. The predefined trust that insiders must be granted requires more sophisticated security measures. The insider threat is related to the level of their sophistication and depends on the users' breadth and depth of knowledge, as well as their finesse [27].

Insiders can trigger either an accidental or malicious threat, i.e., they can intentionally try to cause harm. Information security measures – e.g., encryption, access control, or least privileges principle – must be implemented regarding to human factors, e.g., with personnel checks or focused risk assessments regarding motivation, opportunity and capability [28]. While these insider threats cannot be eliminated, they can be assessed and managed. Users must understand the reasons for security controls in order to ensure their effectiveness. Hence, they may find ways to circumvent technical restrictions they are faced with [25].

A variety of models addresses the insider issue, either concentrating on certain aspects (e.g., end user sophistication [27]) or more holistic in nature [26] [29]. The latter approach incorporates characteristics of the organization, the actor including behavior and attitudes, and the attack itself; overall representing the interdependencies of the different influencing factors [26] [29].

Prior national and international studies on insider security threats [29] [30] [31] have been conducted in the last decade and show the increasing importance of this issue up till now. Despite a good coverage of security policies and measures, the users may obviously work around the controls fulfilling their job objectives in a timely manner. Key issues identified by these studies are data loss prevention, remote information access and the threat against the whole information life cycle. They identified awareness trainings and intensive monitoring measures as effective countermeasures [29] [30] [31].

Working conditions in Austria are regularly measured by the „Work Climate Index", which was first conducted in 1997 by the Institute for Empirical Social Studies in cooperation with the Upper Austrian Chamber of Labor. It has evolved into a longitudinal study since then and aims at capturing the perception of employees concerning their working conditions, and reveals long-term changes in the structure of employment (e.g., increases in precarious employment), evaluates the subjective situation of Austrian employees, and analyses specific subgroups of employees (e.g., women or older employees). Since 2008, the "Work Climate Index" is complemented with the "Austrian Occupational Health Monitor" focusing on questions of subjective work-related health. Both studies are based on 4.000 interviews conducted annually [32] [33] [34] [35]. Key finding of both studies is the relationship between time related stress and working conditions [32, p. 14]. The stress increasing factors are regulations exceeding the common working time hours Monday to Friday from 7 am to 5 pm (especially working on Saturdays or Sundays or at night) or working over-time regularly. Other factors are contributing to time-stress as well, for example permanent contact to customers, high responsibility, permanent surveillance or a lack of support from colleagues [36].

As a further step, our study follows a well-founded approach, combining qualitative question technique for discussion rounds and additionally contrasted by the results of a structured and rather restrictive predefined survey with a significant amount of participants. Despite the fact that human behavior can never be modeled accurately through surveys and the results may not be generalized as conclusive evidence for tactical changes in established organizations, the approach reflects a strongly required combination of work satisfaction with information security principles. Due to the extensive survey and the great random sample of respondents, this work might positively influences a proper methodology analyzing the human risk factor in organizations in future, e.g., heuristics, indicators, conditional relationships etc.

Based on attack types documented in recent publications [12] [14] [16], we have identified a series of major risk factors that contribute to the success of attacks and have consequently derived a targeted list of questions. Some of the most interesting questions that were asked in the study described in this paper are:

- What is the role of ICT security in your company?
- How are security and user guidelines handled?
- What is the current state of awareness among employees?
- Which measures are taken to increase the awareness for ICT security?
- Up to which extent is the private use of company equipment allowed?
- Are there currently any privacy or data loss problems?
- How does the company handle personal data?
- How does the company handle information security?
- Who is responsible for information security in the company?

It is expected that by analyzing the answers to these questions and linking them to attack types, a good assessment of an organization's preparedness for handling attacks can be performed based on organizational vulnerabilities and involving social engineering.

III. Study Design and Setting

The design of the empirical study is based on a well-proven approach that was developed by the Institute for Empirical Social Studies. We decided to use a mixed-method-approach developed by the Institute for Empirical Social Studies. We decided to use a mixed-method-approach [37] and combine quantitative and qualitative aspects of social research, starting with desk research and following up with two focus groups and personal interviews.

A. Desk Research

In the course of the desk research, we analyzed current studies on business crime [19] [38] [39], especially concerning (non-)compliance, fraud and personnel risk. Incidents of business cybercrime have generally been on the rise over the last years. Researchers assume that a large number of unreported incidents exist. Quite often, the perpetrators are among the organization's employees. Nevertheless, these incidents are due to employees' negligence and lack of awareness and not due to intentional or malicious acts. Our study showed that there are some conditions that influence non-compliant behavior: personal traits and moral awareness of an employee, the private situation of an employee; the working conditions, competitive pressure, excessive objective management, lack of internal control, leadership, and organizational culture. Based on these conditions, we derived the security level of the organization and the indicators which determine it. On this basis, we were able to develop suitable interview guidelines as well as questions and answers for the survey. These questions reflect the key aspects for non-compliance as identified in the desk research and based on the answers to these questions conclusions can be made how likely and organization will be affected by non-compliance.

B. Focus Groups

The second part of our study consisted of two focus groups, which took place on 23 and 29 April 2015. In general, a focus group is a moderated discourse method in which a small group of people is stimulated by information input to discuss a specific topic [40, p. 9ff].[41]. This input to get the group discussion started can be provided in form of a short presentation, an image or a website. The goal of a focus group is not to find consensus between the participants but to identify the different aspects of a specific topic.

Focus groups are often used for analyzing different opinions in the group and how participants accept other opinions and evaluate certain measures. A core goal of focus groups is to make use of group dynamics, e.g., to motivate the participants to provide information (the participants' contributions are used as reciprocal stimuli), to take advantage of the collective knowledge (which exceeds the individual intelligence of each participant) and to minimize interviewer or moderator effects by discussing with several participants in a focus group at the same time [42].

In general, and also in the course of our study, a facilitator structures the discussion among the participants of the focus group using an interview guideline. Such a guideline shall ensure that all aspects that are relevant to a topic are addressed during the discussions of the focus group. Additionally, the guideline also increases the comparability of the results of several focus groups that discuss a specific topic. The task of the facilitator is to ensure that all aspects of the interview guideline are covered, all participants are equally involved into the discussion, more quiet and reserved persons are encouraged to participate and not to animate dominant participants that use most of the air time [40, p. 15] [42].

There are no uniform ways to evaluate a focus group [40, p. 17]. In principle, the evaluation may focus either on the process of opinion formation (in this case, sequence and content analyses of the transcripts are used [43]), or on the group output on the content level (in this case, the central topics of the discussion are identified and a description and explanation of the different opinions is collected). For our study, we decided to focus on the content level and thus refrained from producing a verbatim transcription of the discussions, which initially were recorded on tape. Rather, we compiled minutes, which captured the participants' statements but partly already shortened them and in this way introduced our interpretation of these statements. The minutes were evaluated using deductive categories, which were also used to prepare the interview guideline, while remaining open towards any new categories that might result from the discussions [43, p. 91] [44, p. 258]. These categories also form the starting point for the presentation of the results given below.

The participants for the focus groups were selected through theoretical sampling based on the characteristics of individual members [44, p. 258] [45]. In this context, theoretical sampling means that the selection did not happen at random but in relation to characteristics which we considered to be significant in the respective framework [45]. The participants were recruited using the Computer Assisted Telephone Interview (CATI) system owned by the Institute for Empirical Social Studies. The scattering of the participants was improved using so-called "screeners", i.e., short questionnaires which record the characteristics that are relevant for the theoretical sampling. Before the start of the focus group, the participants completed a so-called "re-screener", which once again captured the main characteristics of all participants.

We invited both ordinary employees and persons with management functions to our focus groups. Since the selection was based on a theoretical sampling with characteristics like age, sex, and consumer behavior the aim was to form optimal focus groups with uniformly distributed characteristics. Accordingly, six ordinary employees (three men, three women) aged between 31 to 62 years took part in the first group. The second focus group consisted of eight persons in a management position (six men, two women) aged between 42 and 61 years. The group discussions were based on qualitative questioning techniques and facilitated by a trained person who used a structured interview guideline to guide the discussions, which allowed for an open exchange of opinions. The focus of the group discussions was on security measures, recent critical incidents in the area of information security, and on the relationship between employer and employees. All members described information and communication activities as a main part of their ordinary working routine. The participants received an incentive of 40 Euro to compensate for their expenses and motivate them.

C. Personal Interviews

In parallel to the focus groups, we conducted personal interviews with 891 employees of Austrian companies (53%

men, 47% women) including persons with management function in the period from January to March 2015. These face-to-face interviews were structured by a prepared survey consisting of 48 questions having either several predefined answer possibilities or offering a five-tier rating. The interviewer leads through the questionnaire, explains, discusses and finally documents the participant's answers. Participants were chosen by a multistage random sampling, where Austrian municipalities were grouped by the total number of inhabitants for each federal state and political district. Then, municipalities from each predetermined group were picked randomly. Within these municipalities, eligible households were picked randomly and were then used as samples for finding further addresses. Target persons were exclusively chosen based on their home addresses. Within each target household, members were assigned by random numbers, and only those were interviewed, whose number matched the one provided by the Kish selection grid [46]. Thus, each stage in the selection process of participants was guided by randomization.

The survey covered central issues of job satisfaction, general health situation, satisfaction with corporate management, security measures within the organization as well as ICT security in general. Twenty-five percent of the respondents were aged below 29 years, 34% between 30 and 44 years, and 41% older than 45 years. Each interview with workers (30%), employees (55%) and members of public administration affiliates (15%) took 25 minutes on average and was performed at the respondent's personal domicile. Most of the respondents had completed compulsory education (9%) or with apprenticeship as craftsmen (42%). 16% of respondents had gone to college and passed their school leaving examination, 16% went to college but did not finish it, and 17% had graduated from university. More than three fourths (76%) of respondents are employed full time, the rest worked less than 36 hours per week (24%). The results are shown separately between persons with a leading function (11%) and those without (89%). 39% of the respondents earn less than 1.500 EUR per month, 39% more than 1.500 EUR per month and 22% refused to indicate their salary.

The study design described above was geared both towards obtaining a better understanding of how information security works in companies and towards determining key indicators of non-compliance by indirectly gathering information of employees of Austrian companies. This benchmark approach aimed at obtaining an accurate and undistorted view of employees older than 16 years within Austria across various organizational sizes and business sectors. The research community could now start follow-up projects with the same or a similar study design, which would enable more detailed analysis of one business sector or company size.

IV. MAJOR RESULTS

A. Focus Group Discussions

The members of the focus groups reported on relevant information security incidents in their organizations, e.g., data loss of emails during archiving, loss of business data due to collapse of servers, stealing of material, sensitive information, and electronic equipment, physical damage by fire, perimeter control vulnerabilities, accounting errors due to account number conversion, and phishing. In general, the members of the focus groups point out the need for a balance between scope for development and restrictive measures. Both too much surveillance and the lack of it were considered as problematic. In the following paragraphs, we will discuss the results for the main five topics in further detail.

1) Topic 1: Infrastructure

Guidance for an employee's individual behavior is often replaced by external restrictions that are implemented through technical solutions, e.g., blocking of social media networks, automated logouts, frequently forced password changes, access and/or time cards. Such technical restriction might lead to a regulatory overkill and the employees will find ways to boycott or circumvent these restrictive systems. The majority of the focus group members took a liberal position on surfing the internet for private purposes during working hours. Due to the constantly increasing pressure on employees to fulfill their working objectives, the employer often leaves it up to the employees to decide how much of their time and breaks they spend on surfing the web. Page blocking mechanisms are seen as little effective, since employees can use their smartphones instead of a company desktop computer. Some respondents experience a total "computerization" of the daily work routines as a really threatening scenario. When people are only seen as 'operators' of computers (in the literal sense), this carries social risks. Generally, the members of the focus groups expressed a concern that artificial intelligence might soon dominate human intelligence and human labor might become obsolete.

2) Topic 2: Time Management

Work life balance is the most important prerequisite for healthy, hard-working and rule-abiding employees. Organizations increasingly perform health promotion measures and offer incentives to support work-life balance. Even though such measures make sense, there is also some skepticism towards them. Managers criticize these incentives if they are merely used as a ready-made argument in a (neo-) capitalistic system. The argument is that such incentives do not prevent job losses but disguise a "do more with less"-policy in the organizations. In this context, the technical progress in modern communication technologies can also have negative effects on employees' work life balance. The use of corporate smartphones and notebooks increases the availability of employees for work-related tasks and causes an "always online" feeling among employees, which removes the spatial and systematic barriers between work and personal life.

3) Topic 3: Awareness

Employees are often not familiar with the details of the ICT security policies and code of conduct in their company despite the fact that these form part of their contract. The companies do not offer any dedicated trainings but the ICT regulations are brought to the attention of the employees

when they start their job. However, the published content is not any more up-to-date and thus the employees are not aware of the current regulations.

Data protection is seen in a broader and external context. The more benefits the rules and regulations bring for the employees or the society, they more likely will they follow them. A team operating with information, for example, might adhere to the protection of personal data because it wants that its own personal data is protected in the same way.

4) Topic 4: Surveillance

An excess of surveillance and regulations have a negative impact on the working atmosphere and productivity and creates a defiant attitude among employees. As in a self-fulfilling prophecy, employees provoke exactly those acts that they actually want to prevent. The focus group members agreed that regulations are necessary in sensitive areas and regarding sensitive processes, e.g., data of patients, clients, customers and handling of products or money. Employees and employers share the view that delivery on time is more important than the "objectively" monitored working speed, although employees often have the perception of being too much checked upon.

The loyalty of employees suffers when managers enforce strict time recordings or cancel home office agreements. It is demoralizing for employees if extra hours worked cannot be recorded in the time registration system due to system restrictions. Employees see break recording and break logging by computers as a form of "modern slavery".

5) Topic 5: Personal Interaction

Reactive behavior to handle security incidents is not an appropriate strategy. Punishing employees collectively for the misbehavior of single employees deteriorates morale of all staff. Concerning loyalty, there are synergies: employees trust others if others also trust and appreciate them. Hence, when managers foster team work, actively take over responsibility and select the right personnel, the sense of responsibility among employees grow. Happy employees are good employees. Favorable working conditions are an important precondition for motivated and loyal employees. Good relationships between employees and between employees and their managers, transparent information and communication structures, clear working organization and participation in decision making processes are needed to enhance employees' work and life satisfaction and to minimize psychological problems. It is important for the prevention of non-compliance to avoid unfavorable working conditions, e.g., unfair payment, unfair employment conditions, lack of appreciation by managers, lack of support or mobbing in teams or by managers, and lack of available resources. Against this background, it is important that organizations create a good working condition and a good working environment.

One of the most important tasks of human resource management for the future is to select the "right" employees for the "right" tasks in the organization. Consequently, managers focus on a professional personnel selection process. The integrity of the employees is of key importance and considered to be more important than the integrity of the technical systems, which will never function completely error-free. Selecting the right persons is especially important for management positions, because managers have influence on a company's success and working atmosphere. Bad managers can be a threat to the balance of an organization and thus managers should be selected and assessed carefully. Finally, the focus group discussed on whether more regulations and surveillance have the expected effect.

B. Interviews with prepared survey

The 48 answers of the questions discussed in the 891 personal interviews which were conducted by trained interviewers following a predefined survey can be contrasted to the outcome of the focus groups presented in the section before. Hence, the results are structured along the same five main topics.

1) Topic 1: Infrastructure

15% of the respondents answer to the question how many percent of the employees in the company do the major share of their work on a computer that the percentage is 100% – all employees predominantly use a computer for their work – whereas 12% answer that no one in the company uses a computer for the major share of their work. However, one quarter of the respondents cannot provide further details on this. On average, 56% of the employees predominantly use a computer for their work. There are significant differences between branches, size of the organization and number of sites that an organization has. Smartphone usage shows a similar pattern: 37% of the employees use a smartphone as business phone. In general, using smartphones for work is common in all branches. However, around one quarter of the respondents cannot answer the question and one third say that no smartphones were used as business phones in their company. Similar to the results for computer usage, the share of companies without smartphones is highest in companies with less than 10 employees (49%) and with only one site (39%).

30% of the employees (and 46% of the managers) indicate that the technical equipment provided by the employer may be used for private purposes. It is less common to use private devices for work. However, every fifth respondent indicates that this is allowed in his/her company. The use of private equipment, in particular, has negative implications both for the employees (the line between work and private life gets blurred) and for the companies ("bring your own disaster"). Overall, it can be concluded that, as expected, computers and smartphones form part of the basic equipment of any larger company and that employees (have to) work with them every day. This has led to the situation in the last decade that companies have to deal with the security implications of using these devices. Nowadays, this issue has to be addressed not only by large companies, but increasingly also by small and medium enterprises.

2) Topic 2: Time Management

As shown in Figure 6, one third of the employees answer company emails outside of working hours. Especially managers often can be reached outside of normal working hours: two thirds of them sometimes and 44% several times a week, whereas only 12% of normal employees work

outside of normal working hours. The more the work depends on ICT services, the more the respondents communicate about work after working hours. Around 15% of employees are allowed to work at home. This proportion increases with the level of education: university graduates telework up to 35% of their working hours. The larger the company and the higher the employee's position in the hierarchy, the more likely is the employee to be allowed to work at home.

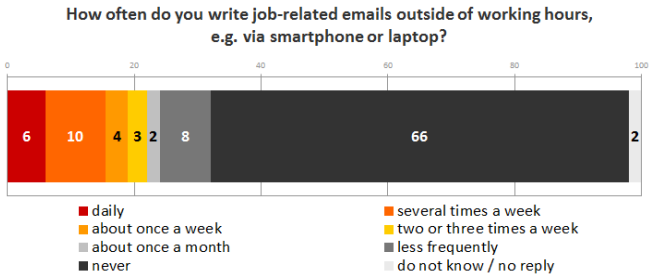

Figure 6. Employees' email communication outside of working hours (values in %; n=891)

35% of the respondents state that their jobs can be reconciled very well with their private interests and family commitments, and 46% think that they can reconcile these things rather well. On the other hand, only 3% of the respondents have the feeling that it is difficult to reconcile their private with their working life. Another 15% of the respondents are indifferent, but this shows that there is room for improvement for the concerned respondents. The group of persons aged 30 to 44 is less satisfied with their work-life balance. This is probably due to the fact that this group typically takes care of small children beside their work. Regarding the effects on human health, the survey shows that time pressure is the major stressor at the work place. Every fifth respondent feels very stressed by it, a quarter of the respondents states that they are moderately stressed by it. 7% feel very stressed and another 13% moderately stressed because work cuts into their leisure time. Both stressors affect managers slightly more than other respondents. The technological developments of the last years contribute to the fact that the line between work and personal life gets more and more blurred. Although these technologies also bring advantages e.g., flexible working arrangements and time management, they also carry risks for employees, e.g., for their health. For the key personnel of an organization these risks tend to be higher.

3) Topic 3: Awareness

More than half of the respondents and three fourths of the interviewed managers consider information security to be an important topic. The survey results indicate that the importance attached to information security grows in line with the size of the organization and has special relevance when the company has offices abroad. Almost 75% of the persons working in large-scale companies (more than 100 employees) assess information security's importance to be very high or high, as shown in Table I. The first row in Table I entitled with "Total" compares the corresponding percentage value without distinction of the organization sizes as reflected by row two to six. The survey also showed that the sensitivity regarding information security is low among employees of very small organizations and of organizations with a low ICT usage.

Table I. Importance of information security divided into company size (n=891)

Company Size (numeric values in %)	very high	high	medium	low	very low	don't know / not specified
Total	28,39	24,55	11,43	5,20	6,90	23,53
Below 10 employees	20,41	17,96	13,87	7,35	13,06	27,35
10 to 19 employees	24,42	26,27	12,44	5,53	5,53	25,81
20 to 49 employees	28,37	27,40	11,54	5,77	6,25	20,67
50 to 99 employees	34,07	30,77	7,69	3,30	3,30	20,87
100 or more employees	47,15	25,20	7,33	0,81	0,81	18,70

Information security was found to have an exceptional standing in companies in the finance and insurance sector (90%), in public administration (77%), and in the health and welfare sector (66%), presumably due to the awareness for processing sensitive data. Nevertheless, one third of the respondents indicate that they have no information security guideline for ICT usage. It is remarkable that especially employees with a lower level of education do not know about any regulations. The information security awareness is comparatively higher in the finance and insurance sector (93%) and in public administration (81%).

A similar picture appears when analyzing the existence of information security awareness measures. Only 28% of respondents report of (semi-)annual measures, 15% indicate that those measures are rarely performed, one third indicate that no such measures are performed, and one fourth of the respondents do not know whether such measures exist. These results indicate that for almost half of the respondent's organizations no awareness activities are in place. This is emphasized by the results about employee's awareness attitude in Figure 7; almost 60% of the respondents see information security awareness attitudes of their colleagues, but on the other hand 40% do not. The main topics addressed by these awareness measures concern the handling of passwords, behavior during information security incidents and using the internet, awareness concerning the sensitivity of the processed data, risks of mobile ICT devices and data storages, contracts with external personnel, and social engineering strategies.

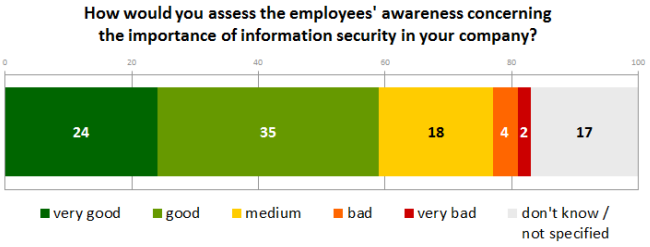

Figure 7. Employees' awareness assessment (values in %; n=891)

Furthermore, the employees are asked how specifically they handle sensitive information and security policies in their organizations. 8% say that employees talk (very) often about sensitive information, also outside the company; whereas 56% indicate that this basically never happens. 7% state that violations of security policies happen frequently, and 6% of the respondents indicate that they do not comply with ICT regulations. On the other hand, 63% and 59%, respectively, state that violations of security policies and violations of the ICT regulations virtually never happen. Figure 8 provides a summarizing sample of explicitly information security related questions and reflects the answers given in the 891 personal interviews. It shows not only the technical implementation of information security measures in the organizations, but in fact the degree of successfully enforcing them because the employees have obviously recognized the information security measures.

Figure 8. How employees handle information security (values in %; n=891)

4) Topic 4: Surveillance

Almost half of the respondents answer that internet and ICT services cannot be used for private purposes, whereas the rest of the respondents are not sure about it. Only 17% of the respondents report that they have an explicit permission to privately use the internet and ICT services provided by their organization. The smaller the organization, the more likely it is that the organization enforces no rules concerning this private use. Companies with offices abroad are more likely to have some rules concerning the private usage of ICT services. Almost three fourths of respondents indicate that there have been no data loss and data protection incidents in their organizations, whereas the rest cannot answer the questions. 86% of the respondents trust their employers concerning the processing of their sensitive data, only 8% do not. The proportion of those who do not trust their employers in this regard is higher in public administration: 18% have doubts whether their organization protects data appropriately. 46% of the respondents know which data his or her employer stores, whereas 45% do not know.

The main proportion of the employees uses working time recording systems, either manual recordings (33%) or an electronic badge (41%). In particular, large-scale enterprises use working time recording and access systems, have special visitor regulations, accounting systems for services or telephone cost monitoring. Video surveillance is more common in the finance and insurance sector, whereas Global Positioning System (GPS) locating is more common in transport services. As illustrated by Figure 9, around 68% of the respondents have no impression that their work place is monitored electronically – this is especially evident for employees from large-scale enterprises. On the other hand, 27% think that they are under surveillance at work.

In companies in Austria, a whistleblower hotline is rather unusual: 72% of respondents report that their organizations have no anonymous hotline, whereas 20% of respondents indicate that they do not know whether such a hotline exists. To conclude, performing a detailed evaluation of a company's information security is rather difficult, since employees are often not allowed to openly speak about security incidents, which results in a considerable number of unrecorded incidents.

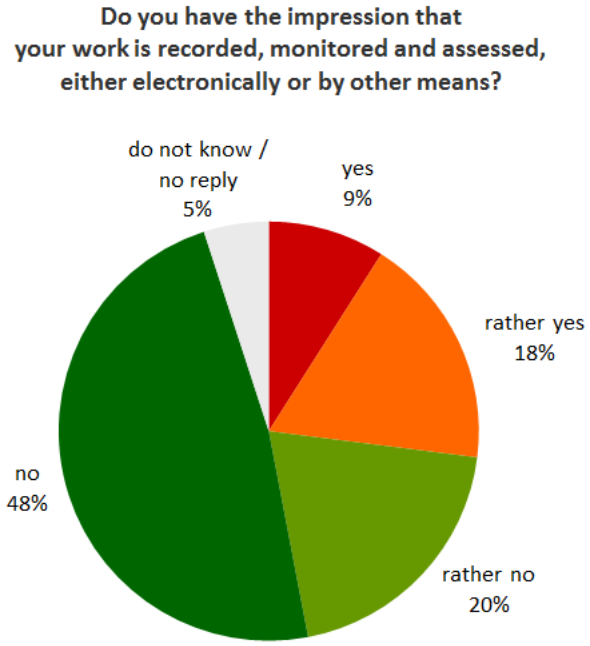

Figure 9. Impression about work surveillance (values in %; n=891)

1) Topic 5: Personal Interaction

The personal interviews with employees generally show that the respondents are most satisfied with the collaboration with their colleagues, the company`s image, the content of their work and the appreciation of their work by colleagues. More than 78% of the respondents and 63% of respondents with only compulsory education as highest education level stated their satisfactions with these aspects. This group indicated comparatively lower satisfaction levels in all categories than the rest of the respondents. Therefore, the satisfaction level of this specific group is explicitly indicated as a second percentage in the following results. Respondents indicated medium satisfaction with their line managers, their individual autonomy to take decisions on their working processes, their working time, and the social policies of the company (more than 66% and 45%, respectively). The respondents were least satisfied with training options, workload, employee participation and potential career possibilities (more than 48% and 33%, respectively).

As depicted in Figure 10, loyalty of employees to their organization is relatively high. If they were to choose again, 72% of the respondents would like to have a job in the same organization. On the other side, 9% would not strive for this. It has to be noted that women show a stronger tendency of choosing the same company again (75%) than men (69%). The results clearly show that with rising age the share of those employees who would strive for a job in the same company decreases. The share of managers that would choose a job in this organization again was above the average share (80%). Two thirds (66%) of the respondents would recommend a job in the organization for which they work. Among mangers the share is 78%. This share of 66% of respondents who would recommend their organization to relatives or friends is relatively high. On the other hand, only almost one out of ten employees would not recommend their organization. The most skeptical groups concerning these questions are persons with compulsory education (14%), persons with a net income less than 1.050 Euro (14%), and employees in companies with offices abroad in other EU countries (13%) and outside the European Union (19%).

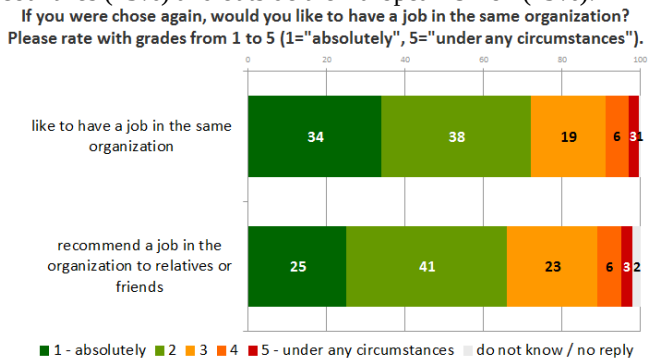

Figure 10. Loyalty of employees to their organization (values in %; n=891)

Furthermore, the interviews showed that seven to eight out of ten employees comply with ICT policies, do not cheat the organization, do not take home data or steal anything, do not harm the enterprise intentionally or unintentionally, do not print private documents and do not talk about sensitive information outside of the work. In contrast, up to 7% have committed at least one of those actions. 14% of employees and 19% of managers go to work when they are ill due to their sense of duty, workload and a lack of deputies. In general, one quarter of the employees states that they went to work at least one day in the past half year although they were having health problems. In contrast, 9% of the respondents indicated that they had stayed at home at least once in the past although they had not been ill.

Respondents considered ICT services to be a key issue in organizations, regardless of the business sector. Almost half of the respondents indicated that company smartphones are an important topic. The proportion of ICT and smartphone usage is considerably higher in organizations with less than ten employees and only one location. 30% of the employees and 46% of the managers are allowed to use the devices privately. Bring your own device (BYOD) is permitted only for one fifth of employees.

The overall handling of information security differs strongly between managers and employees. The knowledge on information security is substantially lower among employees. The probability, that an organization enforces regulations on information security, increases with the size of the organization or if the organization has offices abroad. Again, the finance and insurance sector, public administration and the health and welfare sector are those business sectors in which information security represents an integral part of organizational culture.

It is remarkable to note that only 15% of the respondents indicated that their organization has clearly defined who is responsible for information security, risk and compliance. On the contrary, 54% reported that their organization has not defined this responsibility and 31% did not know. In different organizations, the responsibility is defined in different ways and may lie with the ICT department, a dedicated person who is responsible for information security, an external company, an audit department or the top management. The likelihood, that appropriate responsibilities are established and enforced, increases with the size of the organization and whether the company has offices abroad.

V. CONCLUSIONS

Based on the findings described in Section IV above, we can draw the following top-5-conclusions:

- *High cyber security awareness.*
  The awareness concerning the importance of cyber security is exceptional in the highly sensitive areas, i.e., the Austrian financial and insurance sector (about 90%) and the public administration (about 77%).
- *Poor flow of information.*
  Although security awareness is high among employees, often the responsibilities are not clear. In more than eight out of ten companies it is indistinct who is responsible for information security. Further, one out of three companies does not have a security guideline employees are aware of and in almost 60% of the cases, security awareness measures are either non-existing or not visible for the employees.

- *Strong connection between employees and company*. Employee's loyalty to their company is rather high: roughly, less than one out of ten employees would strive for a job in another company and roughly two out of three managers would recommend a career in their companies to their relatives.
- *Loyal employees are honest employees.* Eight out of ten employees do not cheat the organization, take home important data or steal anything.
- *Sufficient work-life balance is crucial.* Less than one out of 20 employees think that their work-life balance is bad, but already one out of five feels heavily strained due to time pressure, identifying it as a health burden. Technological developments like mobile devices blur the line between work and personal life.

Considered in more detail, our findings show that non-compliance is more likely in an environment that is characterized by poor working conditions These include, among others, inadequate salary, job insecurity, insufficient appreciation of work, lacking support from team members or supervisors, mobbing, and lack of the resources that are necessary to get the work done. Further, competitive pressures, a focus on simplistic success parameters, problems in a company's control system, management style and corporate culture also panders to non-compliant behavior. Favorable working conditions are therefore important in order to enhance the motivation and loyalty of employees [47]. Thus, it is crucial for companies to ensure good working conditions. External regulations and technical solutions, e.g., automated logouts, frequent password changes, access and time badges, are replacing the individual behavioral orientation. Overregulation leads to employees boycotting or bypassing the control system. Excessive control and regulation has a negative impact on the work environment and hampers productivity. Employees often spend working hours with defiant attitudes.

Managers have great influence on the work environment of their employees [48]. Therefore, it is crucial that the managers are selected carefully because they contribute essentially to the company's success and working atmosphere. Good relationships between employees and managers, transparent information and communication structures, transparent work organization and participation in decision-making are necessary to enhance work-life satisfaction and reduce the occurrence of mental disorders. Work life balance in general is considered a requirement for healthy, hard-working, compliant behavior. At the same time, smartphones and laptops enable an integration of work and private life. Nevertheless, the result is that the line between work and leisure is becoming more and more blurred.

While Austrian companies, especially larger ones and also innovative small and medium-enterprises are generally well-prepared concerning information security, the average of small and medium-enterprises still needs substantial support due to a lack of available funding for cyber security measures in order to catch up. Besides the size of the organization, the business sector is decisive for whether information security measures are implemented or not. In sectors where employees are used to handle a lot of sensitive data, such as in the finance and insurance sector, the health sector or the public administration sector, advanced information security measures can be found. Our findings indicate that stronger regulations, monitoring and surveillance measures might not lead to the expected effects in all cases. Consequently, one of the main tasks for human resource management is the selection of loyal employees and the successful integration of employees into the organization.

Hence, the level of information security awareness in Austrian organizations is higher than reflected in the general studies we analyzed [16, p. 5] [17]. Employees are extensively honest. Future research might focus on a comparison of several countries in different cultural areas and within Europe because we expect differences [49]. Another approach we want to follow is to feed an appropriate risk management model with the data presented here. This more systematic research could lead to quantifiable key risk parameters and development of distinct thresholds for the human risk factor of information security. Due to the characteristics of behavior, attitude and perception a heuristic approach could generate input for a scorecard or radar chart with the suggested small set of most interesting questions.

ACKNOWLEDGMENT

This work was partly supported by the European Commission's Project No. 608090, HyRiM (Hybrid Risk Management for Utility Networks) under the 7th Framework Programme (FP7-SEC-2013-1).

REFERENCES

[1] C. Schuster, M. Latzenhofer, S. Schauer, J. Göllner, C. Meurers, A. Peer, P. Prah, G. Quirchmayr, and T. Benesch, "A Study on User Perceptions of ICT Security," presented at the SECURWARE 2016 : The Tenth International Conference on Emerging Security Information, Systems and Technologies, Nice, 2016, pp. 281–288.

[2] M. Plischke, "Company's Prevention: Risk Management Competing with Technology [in German: Unternehmensprävention: Risikomanagement im Wettlauf mit der Technik]," *Inf. Manag. Consult.*, no. 3, pp. 57–60, 2009.

[3] C. Suchan and J. Frank, *Analysis and Design of Powerful IS Architectures: Model-based Methods from Research and Teaching in Practice [in German: Analyse und Gestaltung leistungsfähiger IS-Architekturen: Modellbasierte Methoden aus Forschung und Lehre in der Praxis]*. Springer-Verlag, 2012.

[4] M. Baram and M. Schoebel, "Safety culture and behavioral change at the workplace," *Saf. Sci.*, vol. 45, no. 6, pp. 631–636, 2007.

[5] C. Buck and T. Eymann, "Human Risk Factor in Mobile Ecosystems [in German: Risikofaktor Mensch in mobilen Ökosystemen]," *HMD Prax. Wirtsch.*, vol. 51, no. 1, pp. 75–83, 2014.

[6] F. W. Guldenmund, "The use of questionnaires in safety culture research–an evaluation," *Saf. Sci.*, vol. 45, no. 6, pp. 723–743, 2007.

[7] B. Fahlbruch and M. Schöbel, "SOL–Safety through organizational learning: A method for event analysis," *Saf. Sci.*, vol. 49, no. 1, pp. 27–31, 2011.

[8] Federal Ministry for Transport, Innovation and Technology (BMVIT) and Austrian Research Promotion Agency (FFG), "KIRAS Security Research: MetaRisk," 2016. [Online]. Available: http://www.kiras.at/. [Accessed: 27-Dec-2016]

[9] M. Jakobsson and S. Myers, *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons, 2006.

[10] S. Schiebeck, M. Latzenhofer, B. Palensky, S. Schauer, G. Quirchmayr, T. Benesch, J. Göllner, C. Meurers, and I. Mayr, "Practical Use Case Evaluation of a Generic ICT Meta-Risk Model Implemented with Graph Database Technology," *Int. J. Adv. Secur.*, vol. 9, no. 1 & 2, pp. 66–79, 2016.

[11] Federal Chancellery of Austria, Ed., "Cybersecurity in Austria [in German: Cybersicherheit in Österreich]." Mar-2015.

[12] nic.at and CERT Austria, "Report Internet Security Austria [in German: Bericht Internet-Sicherheit Österreich 2015]." Feb-2016.

[13] Ministry of Finance, Federal Chancellery of Austria, and A-SIT Center for Secure ICT, "ICT Security Portal – Cybermonitor [in German: IKT-Sicherheitsportal – Cybermonitor]," *Onlinesicherheit.at*, 16-Feb-2016. [Online]. Available: https://www.onlinesicherheit.gv.at. [Accessed: 16-Feb-2016]

[14] Bundesamt für Sicherheit in der Informationstechnik (BSI), "The Situation of IT Security in Germany 2015 [in German: Die Lage der IT-Sicherheit in Deutschland 2015]." Nov-2015.

[15] Bundeskriminalamt Wiesbaden, "Cybercrime Federal Overview 2014 [in German: Cybercrime Bundeslagebild 2014]." Bundeskriminalamt Wiesbaden, 2014.

[16] Information Systems Audit and Control Association (ISACA), Ed., "State of Cybersecurity: Implications for 2015 - An ISACA and RSA Conference Survey." 2014.

[17] Information Systems Audit and Control Association (ISACA), Ed., "State of Cybersecurity: Implications for 2016 - An ISACA and RSA Conference Survey." 2016 [Online]. Available: https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf. [Accessed: 03-Jan-2017]

[18] G. Cluley, "Hackers Steal $55 million From Boeing Supplier," 21-Jan-2016. [Online]. Available: http://www.tripwire.com/state-of-security/security-data-protection/boeing-supplier-hacked-claims-55-million-worth-of-damage-as-stock-price-falls/. [Accessed: 16-Feb-2016]

[19] Pricewaterhouse Coopers, "Economic crime: A threat to business processes - PWC´s 2014 Global Economic Crime Survey - US Supplement." 2014.

[20] Pricewaterhouse Coopers, "Adjusting the Lens on Economic Crime: Preparation brings opportunity back into focus - Global Economic Crime Survey 2016: US Results." 2016 [Online]. Available: https://www.pwc.com/us/en/forensic-services/assets/gecs-us-report-2016.pdf. [Accessed: 03-Jan-2017]

[21] H. Quentmeier, *Practice Manual Compliance: Fundamentals, Objectives, and Practical Advice for Non-lawyers [in German: Praxishandbuch Compliance: Grundlagen, Ziele und Praxistipps für Nicht-Juristen]*, 1. Aufl. Wiesbaden: Gabler, 2012 [Online]. Available: B:DE-101 application/pdf http://d-nb.info/1018131469/04 DNB-TOC Inhaltsverzeichnis 2

[22] W. Schettgen-Sarcher, S. Bachmann, and P. Schettgen, *Compliance Officer*. Wiesbaden: Springer Fachmedien Wiesbaden, 2014 [Online]. Available: http://dx.doi.org/10.1007/978-3-658-01270-0 Resolving-System Volltext

[23] Semmer, N., "Stress," in *Handwörterbuch Arbeitswissenschaft*, H. Luczak and W. Volpert, Eds. Stuttgart: Schäffer-Poeschl, 1997, pp. 332–339.

[24] R. Raml, "Positive indicators for health in context of work: an interdisciplinary extension of the term health and its consequences for the differentiation of health situations for employees [in German: Positive Indikatoren der Gesundheit im Kontext Arbeit: eine interdisziplinäre Erweiterung des Gesundheitsbegriffs und dessen Folgen für die Differenzierung gesundheitlicher Lagen bei unselbständig Beschäftigten]," Medizinische Universität, 2009.

[25] C. Colwill, "Human factors in information security: The insider threat–Who can you trust these days?," *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 186–196, 2009.

[26] J. R. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in *Security and Privacy Workshops (SPW), 2014 IEEE*, 2014, pp. 214–228.

[27] G. B. Magklaras and S. M. Furnell, "A preliminary model of end user sophistication for insider threat prediction in IT systems," *Comput. Secur.*, vol. 24, no. 5, pp. 371–380, 2005.

[28] J. Hunker and C. W. Probst, "Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques.," *JoWUA*, vol. 2, no. 1, pp. 4–27, 2011.

[29] A. M. Munshi, "A study of insider threat behaviour: developing a holistic insider threat model," 2013.

[30] RSA, "The Insider Security Threat in I.T. and Financial Services: Survey Shows Employees' Everyday Behavior Puts Sensitive Business Information at Risk." RSA, 2008.

[31] L. Tan, *Asia worried about insider threat. ZDNet Asia*. 2008.

[32] R. Raml, Ed., "Working conditions and stress: findings of the Austrian Work Climate Index [in German: Arbeitsbedingungen und Stress: Erkenntnisse aus dem österreichischen Arbeitsklima Index]," *Schriftenreihe Österr. Arbeitsklima Index - Austrian Work Clim. Index*, vol. Arbeitsbedingungen und Stress, no. 3, pp. 12–17, 2015.

[33] R. Raml, "Scientific fundamentals of the Austrian Occupational Health Monitor [in German: Wissenschaftliche Grundlagen des Österreichischen Arbeitsgesundheitsmonitors]," *Schriftenreihe Österr. Arbeitsklima Index - Austrian Work Clim. Index*, no. 2, pp. 12–19, 2012.

[34] R. Raml, "A theoretical evaluation of the Work Climate Index [in German: Eine theoretische Evaluierung des Arbeitsklima Index]," *Schriftenreihe Österr. Arbeitsklima Index - Austrian Work Clim. Index*, no. 1, 2009.

[35] R. Raml and A. Schiff, "The localization of the Work Climate Index in a sociologic, psychologic and economic

theory spectrum [in German: Die Verortung des Arbeitsklima Index im soziologischen, psychologischen und ökonomischen Theorienspektrum]." 2016.

[36] M. Tarafdar, Q. Tu, B. S. Ragu-Nathan, and T. S. Ragu-Nathan, "The impact of technostress on role stress and productivity," *J. Manag. Inf. Syst.*, vol. 24, no. 1, pp. 301–328, 2007.

[37] R. B. Johnson, A. J. Onwuegbuzie, and L. A. Turner, "Toward a definition of mixed methods research," *J. Mix. Methods Res.*, vol. 1, no. 2, pp. 112–133, 2007.

[38] A. V. Heerden, F. Weller, and G. Weidinger, "Business Crime. Gemrany, Austria, Switzerland in comparison. Business Crime in large-sized organizations and medium-sized business [in German: Wirtschaftskriminalität. Deutschland, Österreich, Schweiz im Vergleich. Wirtschaftskriminalität in Großunternehmen und dem Mittelstand]." KPMG, 2013.

[39] Pricewaterhouse Coopers, "Business Crime 2011. Security Situation in Austrian companies [in German: Wirtschaftskriminalität 2011. Sicherheitslage in österreichischen Unternehmen]." PWC, 2011.

[40] M. Schulz, "Quick and easy!? Fokusgruppen in der angewandten Sozialwissenschaft," in *Fokusgruppen in der empirischen Sozialwissenschaft*, Springer, 2012, pp. 9–22.

[41] D. Morgan, *Focus Groups as Qualitative Research*. 2455 Teller Road, Thousand Oaks California 91320 United States of America: SAGE Publications, Inc., 1997 [Online]. Available: http://methods.sagepub.com/book/focus-groups-as-qualitative-research. [Accessed: 03-Jan-2017]

[42] D. W. Stewart and P. N. Shamdasani, *Focus groups: Theory and practice*, vol. 20. Sage publications, 2014.

[43] U. Flick, *The SAGE handbook of qualitative data analysis*. Sage, 2013.

[44] U. Flick, "Qualitative Social Research-An Introduction [in German: Qualitative Sozialforschung–Eine Einführung]," *Reinbek Bei Hambg. Rowohlt*, no. 5th edition, Nov. 2012.

[45] C. Auerbach and L. B. Silverstein, *Qualitative data: An introduction to coding and analysis*. NYU press, 2003.

[46] L. Kish, "A procedure for objective respondent selection within the household," *J. Am. Stat. Assoc.*, vol. 44, no. 247, pp. 380–387, 1949.

[47] B. Aziri, "Job satisfaction: A literature review," *Manag. Res. Pract.*, vol. 3, no. 4, pp. 77–86, 2011.

[48] J. P. De Jong and D. N. Den Hartog, "How leaders influence employees' innovative behaviour," *Eur. J. Innov. Manag.*, vol. 10, no. 1, pp. 41–64, 2007.

[49] Z. Aycan, R. Kanungo, M. Mendonca, K. Yu, J. Deller, G. Stahl, and A. Kurshid, "Impact of culture on human resource management practices: A 10-country comparison," *Appl. Psychol.*, vol. 49, no. 1, pp. 192–221, 2000.