A Study on User Perceptions of ICT Security

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

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

Johannes Göllner, Christian Meurers,
Andreas Peer, Peter Prah
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

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 risk factor is a decisive factor in information security but has still not been fully integrated into information security programs and risk management approaches. Based by this lack of integration, we have designed a study on user attitudes to information security issues in Austrian companies. The survey that has been carried out within this study is based on extensive literature research on risk, behavior and trust models. The analysis of the results comprises 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 vital role of trust in an organization's information and communication technology (ICT) systems has been amply discussed in the literature from various perspectives [1][2]. The attitude of employees as an indicator of emerging problems has also been described in recent publications [3][4]. 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 [5][6].

As part of the KIRAS MetaRisk project [7], originally initiated by Johannes Göllner, supported and partially financed by the Austrian National Security Research Program KIRAS, we conducted a survey 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. Key topics covered by this survey were how individual staff members applied the safeguards that have been set up, how employees treat security-relevant incidents – especially activities to avoid or circumvent those incidents including activities that cause harm to the organization – and 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. With more sophisticated forms of attacks, for example advanced persistent threats (APT) where perimeter controls substantially lose their protective effectiveness [8], 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 cyber-crime is rising [1][6]. 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 2, we first present the scientific basis from the relevant literature and our motivation for the study. Section 3 describes the applied methodological approach of the survey performed for the study. In Section 4, we discuss the main results of the study compared to retrospectively documented attack stories from real life. Section 5 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 [9, p. 8][10][11] and Germany [12][13, 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 [14], shows which types of attacks were most successful in affected enterprises (Figure 1). In this context, phishing attacks had the highest success rate, followed by the classic attack types “malware” and “hacking attempts” and by “social engineering”. The Austrian internet security report 2015 [10, p. 45] 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.

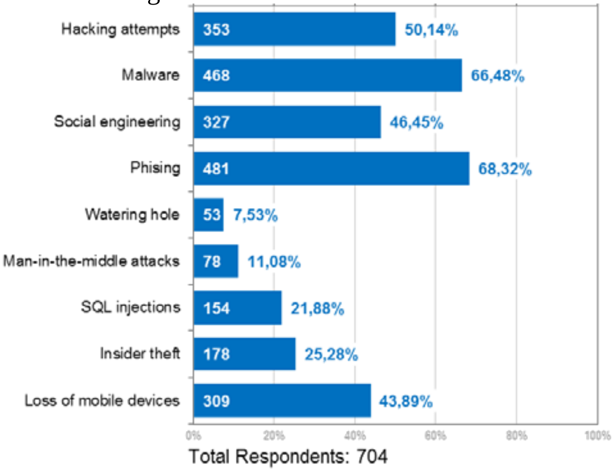

Figure 1. Successful attack types in affected respondent’s enterprises in 2014 [14, p. 6]

As these attacks have a significant financial impact on affected companies [14], 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 has recently caused an estimated damage of 50 million EUR [15]. To emphasize this financial aspect, Figure 2 points out that almost 50% of US companies suffer financial damage from attacks at least annually, while at the same time employees and managers are more and more ignorant of the impacts of cybercrime.

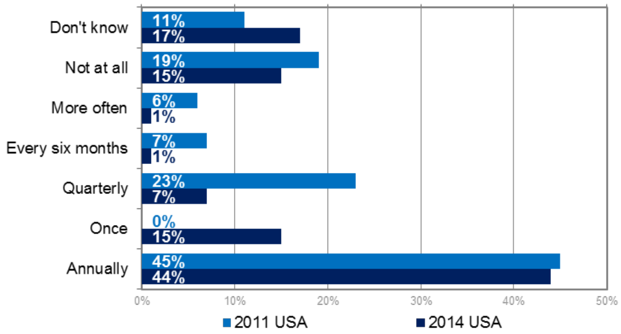

Figure 2. Relative financial impact of cybercrime on organizations [16, p. 28]

Figure 3 clearly shows that insiders – no matter whether they have malicious or non-malicious intents – have made a significant contribution to the damage that enterprises suffered in 2014.

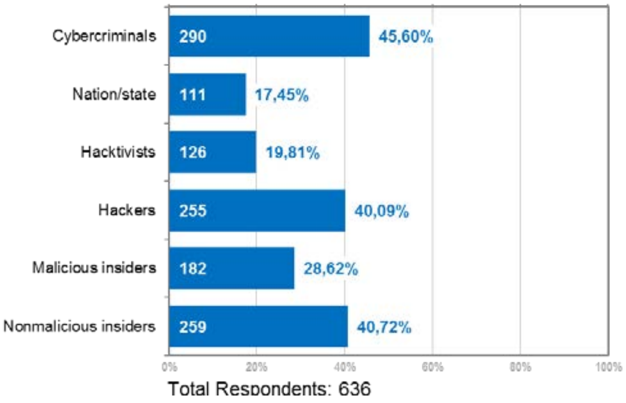

Figure 3. Threat actors [14, p. 5]

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 [17]. 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 [18, 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 [18, p. 233ff].

In general, working conditions can be divided into three categories; macro, meso and micro level [19]. Raml [20, 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 [20]. 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 [20]. 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 [22][23][24]. 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 [24].

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. 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 [22].

A variety of models addresses the insider issue, either concentrating on certain aspects (e.g., end user sophistication [24]) or more holistic in nature [23][25]. 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 [23][25].

Prior national and international studies on insider security threats [25][26][27] 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 [25][26][27].

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 [28][29][30][31]. Key finding of both studies is the relationship between time related stress and working conditions [28, 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.

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 [10][12][14], 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

Regarding the design of the study, we followed a well-proven approach that was developed by the Institute for Empirical Social Studies. We decided to use a mixed-method-approach and combine quantitative and qualitative aspects of social research, starting with desk research and following up with two focus groups and questionnaires.

In the desk research, we analyzed current studies on business crime [32][33][34][35], especially concerning (non-)compliance, fraud and personnel risk and summarized key findings. Cases of Business Cybercrime generally have risen over the last years and researchers assume a large estimated number of unreported cases. The offenders are quite often the own employees of an organization, not only caused by intentional acting but carelessness and lack of awareness. We found out that there are some conditions promoting non-compliant behavior: personal characteristics, the own moral awareness, individual situation on a personal level; work conditions, competitive pressure, excessive objective management, lack of internal control, leadership, and organizational culture. Based on these aspects, we derived the security level of the organization and the indicators which determine it. Thus, we were able to develop appropriate interview guidelines as well as questions and answers for the survey. These questions reflect identified key aspects whether an organization is affected by non-compliance more likely or not.

For two focus groups that took place on April 23rd and 29th 2015 we invited both ordinary employees and persons with management functions. The selection process for the participants in the focus groups had two stages and was in line with internal quality standards of the Institute for Empirical Social Studies in order to form optimal focus groups with uniformly distributed attributes, e.g., age, sex, and consuming behavior. In the first group, six ordinary employees (three men, three women) aged between 31 to 62 years took part. The second focus group consisted of eight persons in management position (six men, two women) aged between 42 and 61 years. The group discussions were based on qualitative question techniques and moderated by trained persons following a structured interview guideline, which allowed for an open exchange of opinions. We emphasized on security measures, recent incidents critical for information security, and on the relationship between employer and employee. All members described information and communication activities as main part of their ordinary working routine.

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, we randomly picked eligible households that again were 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 [21]. 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

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. The members of the focus groups generally 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. The loyalty of employees suffered when managers enforced strict time recordings, cancelled home office arrangements, and collectively punished employees for the misbehavior of single employees. In contrast, when managers fostered team work, actively took over responsibility and selected the right personnel the sense of responsibility among employees grew.

The personal interviews with employees show that the respondents are most satisfied about the collaboration with their colleagues, the company`s image, the content of their work and the appreciation of their work by colleagues – it is reflected by more than 78% – and 63% of persons with only compulsory education (the latter group reveals comparatively lower values than for the others and is explicitly represented by the second percentage quotation in the following). 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).

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 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.

One third of the employees answers 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. The proportion raises 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.

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 that is 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 1. 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. The first row in Table 1. entitled with "Total" compares the corresponding percentage value without distinction of the organization sizes as reflected by row two to six.

Table 1. 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 indicated 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 reported of (semi-)annual measures, 15% indicated that those measures are rarely performed, one third indicated that no such measures are performed, and one fourth of the respondents did 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 5; 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.

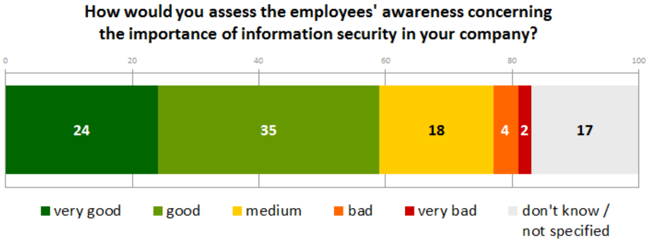

Figure 4. Employees' awareness assessment (values in %; n=891)

Almost half of the respondents answered that internet and ICT services cannot be used for private purposes, whereas the rest of the respondents were not sure about it. Only 17% of the respondents reported 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 indicated that there have been no data loss and data protection incidents in their organizations, whereas the rest could not 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. 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 indicated that their organizations have no anonymous hotline, whereas 20% of respondents indicated that they do not know whether such a hotline exists. 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 forms an integral part of organizational culture.

It is remarkable to note that only 15% of the respondents indicated that their organization has defined who is responsible for information security, risk and compliance, whereas 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 likeliness, that appropriate responsibilities are established and enforced, increases with the size of the organization and if the company has offices abroad.

Future research might focus on a comparison of several countries in different cultural areas and within Europe. 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.

V. Conclusions

Our findings show that non-compliance is more likely in an environment that is characterized by poor working conditions (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), competitive pressures, focus on simplistic success parameters, and problems in a company's control system, management style and corporate culture. Favorable working conditions are therefore important in order to enhance the motivation and loyalty of employees. 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. 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 necessary requirement for healthy, hard-working, compliant behavior. At the same time, smartphones and laptops enable an integration of work and private life.

The result is that the line between work and leisure is becoming more and more blurred.

Although Austrian companies are in general well-prepared concerning information security, the small and medium-enterprises will have to increase their efforts 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.

REFERENCES

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

[2] 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.

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

[4] 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, 2014, pp. 75–83.

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

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

[7] 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: 17-Feb-2016].

[8] S. Schiebeck, et.al., “Implementation of a Generic ICT Risk Model using Graph Databases,” presented at the SECURWARE 2015, 9th International Conference on Emerging Security Information, Systems and Technologies, Venice, Italy, 2015, pp. 146–153.

[9] Federal Chancellery of Austria, Ed., “Cybersecurity in Austria” [in German: “Cybersicherheit in Österreich”], Mar-2015.

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

[11] 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].

[12] 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.

[13] Bundeskriminalamt Wiesbaden, “Cybercrime Federal Overview 2014“ [in German: “Cybercrime Bundeslagebild 2014”], Bundeskriminalamt Wiesbaden, 2014.

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

[15] 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].

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

[17] 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. Edition. Wiesbaden: Gabler, 2012.

[18] W. Schettgen-Sarcher, S. Bachmann, and P. Schettgen, Eds., Compliance Officer: The Augsburg Qualifying Model [in German: Compliance Officer: das Augsburger Qualifizierungsmodell], Wiesbaden: Springer Gabler, 2014.

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

[20] 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”], Medical University, 2009.

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

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

[23] 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.

[24] 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, 2005, pp. 371–380.

[25] A. M. Munshi, A study of insider threat behaviour: developing a holistic insider threat model, Ph.D. Curtin University, School of Information Systems, 2013

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

[27] L. Tan, “Asia worried about insider threat. ZDNet Asia.“, 2008.

[28] R. Raml, “Working conditions and stress: findings of the Austrian Work Climate Index“ [in German: “Arbeitsbedingungen und Stress: Erkenntnisse aus dem österreichischen Arbeitsklima Index”] in “Arbeitsbedingungen und Stress” - Schriftenreihe Österreichischer Arbeitsklima Index 3, 2015, S 12-17

[29] R. Raml, “Scientific fundamentals of the Austrian Occupational Health Monitor“ [in German: “Wissenschaftliche Grundlagen des Österreichischen Arbeitsgesundheitsmonitors”] in Schriftenreihe Österreichischer Arbeitsklima Index 2 - Austrian Work Climate Index, 2012, S 12-19

[30] R. Raml, “A theoretical evaluation of the Work Climate Index“ [in German: “Eine theoretische Evaluierung des Arbeitsklima Index“] in ”Schriftenreihe Österreichischer Arbeitsklima Index 1 - Austrian Working Climate Index”, 2009

[31] R. Raml, 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

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

[33] KPMG, “Wirtschaftskriminalität. Deutschland, Österreich, Schweiz im Vergleich. Wirtschaftskriminalität in Großunternehmen und dem Mittelstand.” 2013.

[34] 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.

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