Psychosocial Risks: Can Their Effects On The Security of Information Systems Really Be Ignored?

E. D. Frangopoulos[1], M. M. Eloff[1] and L. M. Venter[2]

[1]School of Computing, University of South Africa (UNISA), Pretoria, South Africa
[2]Director: Research Support, North-West University, South Africa
e-mail: vfrangopoulos@hol.gr; e-mail: eloffmm@unisa.ac.za;
lucas.Venter@nwu.ac.za

Abstract

Psychosocial risks at the workplace is a well-researched subject from a managerial and organisational point of view. However, the relation of psychosocial risks to Information Security has not been formally studied to the extent required by the gravity of the topic. An attempt is made to highlight the nature of psychosocial risks and provide examples of their effects on Information Security. The foundation is thus set for methodologies of assessment and mitigation and suggestions are made on future research directions.

Keywords

Information Security, Psychosocial Risks

1. Introduction

It has been well established in the standard literature that major vulnerabilities of Information Systems can be attributed to their human element, i.e. the users. When these users are themselves targeted, the compromise of information security becomes imminent, irrespective of technical measures that strengthen information security as well as physical security. In previous work, it was shown that there are many human psyche aspects that attackers can use effectively against any user they set their sights on (Frangopoulos et al., 2010). Social aspects of Information Security were also examined (Frangopoulos et al., 2008) and their significance in successful attacks was discussed. In addition to breaches caused by such attacks, one must also not overlook those insider security incidents that are caused deliberately or accidentally, where due to user action, negligence, fault or oversight, information security is ultimately compromised. This again has to do with the fact that Information System users are humans with individual abilities and shortcomings that cannot be categorised and dealt with in bulk from an Information Security point of view. In this context, even though "to err is human", when these errors -deliberate or not- are aggravated by psychosocial factors, there may be dire consequences on Information Security. Hence, ways must be found to reduce such occurrences by ensuring that the causal factors of psychosocial risks that are inevitably present in any modern organisation are effectively controlled.

Social sciences have been dealing with the field of psychosocial risk mitigation for many years and no course in business management disciplines can be deemed complete without proper reference to this issue. The obvious conclusion is thus that if psychosocial factors affect all forms of business operations and a clear concern exists on how to control these factors and reduce their adverse effects, then it is only reasonable to assume that the security of Information Systems, viewed from this angle, is also exposed to risks of a psychosocial nature. This paper identifies psychosocial risks that affect Information Security, shows how this effect comes about and suggests ways and research directions for the assessment and mitigation of such risks.

2. Background

The term "Psychosocial" itself has two components: "Psyche" which pertains to one's own psychological predispositions and "Social" which has to do with external factors, stemming from the role of the individual in society and the interaction with others. By combining the two notions into one term and using it to describe risk, the emphasis is placed on those risks that result from the individual's own perceptions and psyche as he/she reacts to stimuli from his/her societal environment.

The currently prevailing notion of system security from a systems engineering perspective, as presented by Larson et al. (2009, p.114), is that system security (along with system safety) is yet another design constraint which "*relates to attributes that enable the system to comply with regulations and standards*". Clearly, by adding the intricate parameter of Psychosocial Risk into the equation of Information Systems security, the above notion becomes insufficient. This, however, does not mean that, in designing a more secure system, one has to do away with standards and start from scratch. The standards are there and should be followed as they provide commonly acceptable and effective solutions to a number of different security problems. In a holistic approach to the Information Security issue however, standards should be complemented by those techniques and practices that mitigate risks of a psychosocial nature. In such a holistic approach, the people and their individual characteristics cannot be ignored. Designing secure Information Systems and applications becomes a much more intricate exercise when the individual problems of potential users that may affect Information Security need to be pro-actively addressed. In Bruce Schneier's own words: "*...the mathematics are impeccable, computers are vincible, the networks are lousy and the people are abysmal. I've learned a lot about the problems of securing computers and networks, but none that really helps solve the people problem*" (Schneier, 2004, p.255).

Barring a handful of researchers such as Greitzer et al. (2010; 2010a; 2011) and Vyhmeister et al. (2006) who deal with psychosocial risks in the particular context of Information Security, limited work has been done in this direction. Hence, it would be prudent to set the ground for the current work by examining the idea of psychosocial risks (or "psychosocial hazards" – the two terms seem to be used without distinction in the literature) from the usual managerial and organisational points of view, where extensive research has been and is being carried out.

The International Labour Organisation defines "psychological factors" in terms of the interactions between employee's skills and needs on one side, and job content, work organisation, work management and environmental and organisational conditions, on the other. In this context, "psychosocial hazards" refer to those of the above interactions that have a hazardous influence over employees' health, through the employees' perceptions and experience (ILO, 1986).

Cox (1993) considers that psychosocial hazards may have a direct or indirect adverse effect on both psychological and physical health, through the experience of stress. In a more recent work, he presents a definition for psychosocial hazards as "*those aspects of the design and management of work, and its social and organisational contexts, that have the potential for causing psychological or physical harm*" (Cox et al., 2003, p.195).

Haubold (2008, p.7) defines "psychosocial risks" as the human tensions potentially generated by the application of enterprise strategy. She continues by identifying some of these tensions as stress, the impression of being harassed, violence (in all forms), mental burden etc. In the same text, the author lists a few positions on psychosocial risks adopted by respected researchers in the field, which are included here in order to set the foundation for further discussion:

1. Employee satisfaction determines employee punctuality or absence (Spector, 1997, p.104).
2. Half of the days of absence from work are due to a problematic work environment or stress (Cooper, 1994).
3. Personnel involvement is associated with low running costs and high performance (Mathieu and Zajac, 1990).
4. Employee satisfaction is directly related to client satisfaction (Heskett et al., 1997, p.320)
5. Job satisfaction is founded on personnel involvement. (Vandenberg et al., 1999)
6. Employee satisfaction stemming from job security, compensation and satisfaction in general are directly related to the financial performance of the enterprise. (Schneider et al., 2003)

One has to bear in mind that the above statements view psychosocial risks from a business management angle but, nevertheless, conclusions can be drawn for the research at hand. It is immediately visible though, that if steps are taken to minimize psychosocial risks and keep employees happy, the enterprise benefits.

In order to further highlight the gravity of psychosocial risks, it suffices to mention that according to the European Agency for Health and Safety at Work, one third of the European worker population (i.e. more than 40 million people) report that they are affected by stress at work (EASHW, 2002). On this basis, psychosocial risks are currently recognised as a major challenge to occupational health and safety (EASHW, 2007). In 2007, 13.6% of all workers who responded to surveys carried out in the U.K. by the Health & Safety Executive, when asked to rate how stressful

they felt their job was, reported that they found their job either very or extremely stressful (Webster, 2007). From these three statements, in conjunction to the list of accepted positions regarding psychological risks above, it becomes evident that, up to one third of an enterprise's workforce, could conceivably pose a significant threat to the enterprise's prosperity because of exposure to psychosocial risks.

It is interesting to note that from a managerial and organisational point of view, the issue of psychological risks at the workplace is well-established and well-researched. Furthermore, its importance to the well-being of the organisation is highlighted. However, from the extensive bibliographical research carried out in the course of the present work, only a handful of publications were found to relate psychosocial risks with Information Security in general, and the security of Information Systems in particular. It seems that even though some effort is invested on the general human aspect of Information Security, only a small group of scientists, primarily led by Greitzer, investigates psychosocial risks as a significant factor of Information Security in an effort to mitigate insider threat (Greitzer et al., 2010; 2010a; 2011).

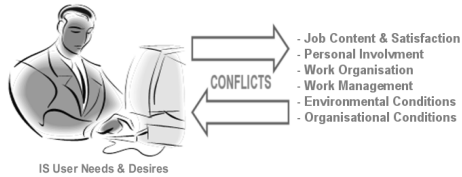

Figure 1: Psychosocial Risks affecting Information Systems users

The conclusion to be drawn is hence that Psychosocial Risks, being such an important factor in the general well-being of an enterprise, can and must not be ignored in the context of Information Security.

3. Common causes and general effects of psychosocial risks

Irrespective of the *nature* of the effects of Psychosocial Risks on the various aspects of an enterprise's prosperity, the *causes* of Psychosocial Risks have been thoroughly investigated in the past. Even though new causes may appear as society and technology progress, there already is a well-defined foundation that can work as the basis for the scope of this paper.

The International Labour Organisation in its invitation to "The New SOLVE" conference (ILO, 2011), lists the following among factors which place high emotional demands at work and contribute to work-related stress:

- Downsizing and outsourcing
- Greater need for flexibility both in functions and skills
- Increasing temporary contracts
- Greater job insecurity
- Higher workloads
- Long working hours
- Work intensification
- Poor work-life balance

Obvious and immediate results of the psychosocial risks caused by the above factors are absenteeism, diminution of employee efficiency and decrease in productivity. Second-order results vary from excessive drinking and smoking, drug abuse, eating and sleep disorders to workplace violence. Another interesting fact is that workers of all categories and occupations are affected, both in developing and developed countries (ILO, 2011).

According to Brun (2003), the psychosocial risks at work can be attributed to events taking place in the private life of the individual, in the organisation where he/she works or in the society in which he functions and progresses. Causal factors of psychosocial risks are also listed as:

- Quantitative work overload
- Qualitative work overload
- Lack of esteem by peers
- Job instability
- Lack of career advancement
- Insufficient compensation for given skills and professional experience
- Poor relations with superiors
- Poor relations with colleagues
- Poor relations with clients
- Lack of participation at the organisational level
- Lack of participation at the individual's level
- Lack of information flow at the organisational level
- Lack of participation at the individual's level
- Insufficient workload
- Unrealistic time constraints
- Conflict of work roles
- Work role ambiguity
- Lack of autonomy
- Lack of decision-making power
- Difficulties in the work environment and the working conditions
- Irregular working hours
- Extended working hours
- Centralised organisational structure

To these, Michie (2002) adds:

- Lack of breaks during work
- Lack of variety in work
- Poor physical work conditions (light, space, temperature etc)
- Working far away from home
- Taking work home
- Job relocation

Other lists of causes of psychosocial risks were also found during the relevant research, but, generally speaking, they revolve around the same themes as above. A detailed comparative description of such causes lies beyond the scope of this work

and the interested reader is directed towards the bibliography presented in the references section of this paper.

It is noteworthy that as the design of Information Systems influences job design and workflow, management practices, organizational policy and other issues, it may itself constitute a causal factor of psychological distress (Vyhmeister, 2006) and, hence, psychosocial risk.

Irrespective of cause, psychosocial risks lead to a variety of problems, many of them quite serious and complex in nature. Haubold (2008, p.14) presents a table of such consequences, which is compiled to show the relations between different manifestations of various problems:

Physical consequences	***Psychological Consequences***	***Behavioural Consequences***
Headaches	Depressive mood	Absenteeism
Sleep disorders	Despair	Drug addiction
Muscular tension	Annoyance	Drug abuse
Weight issues	Anxiety	Sexual problems
Gastrointestinal disorders	Memory lapses	Impatience
Elevated blood pressure	Dissatisfaction	Aggressiveness
Allergy	Frustration	Alimentary problems
High cholesterol levels	Irritability	Drop in creativity and in taking initiatives
Skin conditions	Discouragement	Poor interpersonal relations
	Pessimism	Frequent mood swings
		Superficial relations
		Limited tolerance of frustration
		Disinterest
		Isolation

Table 1: Consequences of Psychosocial Risks

As expected, any of the above may lead to errors, reduction in productivity and sick-leave. Other outcomes are diminished job-satisfaction and commitment, generally unsafe behaviour at the workplace and an increased propensity for accidents (Cooper et al., 1997). To make matters worse, many of these issues are interrelated and often co-exist (Probst et al., 2008).

4. Effects on information security

Having established the gravity of the general effects of psychosocial risks, given that the people who are subject to these may be the users of information systems and thus the handlers of information, it becomes evident that Information Security is directly affected.

Whether intentional or by accident, breaches of Information Security in this context fall under the general category of "insider threat". The person directly or indirectly responsible for such a breach, is by definition an employee of the organisation who, out of malice or because of plain disregard for Information Security rules, allows information to be compromised.

According to recent data breach studies, insiders may directly or indirectly be behind a significant percentage of breaches, whether intentional or not (Verizon, 2009; 2010; 2011). The reported insider threat percentages varied from 17% to 48% of all data breach cases that were studied in the three-year period from 2009 to 2011. The significant fluctuation in the obtained percentages is due to the nature and total volume of the data breach cases examined each year (Verizon, 2011). However, even at the minimum level of 17%, insider threat is still quite substantial and must be examined, analysed and controlled.

In this context, an employee experiencing diminished job satisfaction becomes less committed to the organisation or enterprise he/she works for and may use the enterprise's confidential information as a bargaining chip for alternate employment by a competitor, or, simply, for monetary gain. For an employee who has become indifferent to his/her work, it will be very difficult to go through the sometimes tedious processes to ensure Information Security. Hence, when shortcuts are taken and security rules are not followed, information becomes liable to compromise. For those users afflicted by the physically debilitating consequences listed in table 1, it becomes evident that the employee's judgement may become erratic and accidents will inevitably follow. Insofar Information Security is concerned, accidents such as using an insecure channel to distribute sensitive information can be detrimental.

In order for Information Security policies to be effective, the co-operation of end-users is of paramount importance. When the end-users' abilities and will to co-operate towards better Information Security are curtailed as a direct effect of psychosocial risks, Information Security policies are bound to fail in some degree. It has already been shown that Social Engineering attacks play a major role in Information Security (Frangopoulos, 2007). In order to withstand such an attack, the end-user must be in a state of alertness. This state is impossible to attain under the light of most of the consequences of psychosocial risks listed in table 1.

In order to deal with attacks against Information Security in a centralised way, it is important to have an incident co-ordination and response centre. This centre relies on information from automated systems such as Intrusion Detection Systems and analyses of system log files. In addition to that, an important contribution comes in

the form of feedback on attacks (even attempted ones) received from users. Hence, if the users' ability to contribute in this manner is impeded, the centre's function will be inherently limited.

Poor man-machine interface design on an otherwise secure information system or application may also lead to the compromise of Information Security. The users affected by psychosocial factors, who are already burdened by the interface's bad design and the required time-consuming sequences of actions, when they find themselves pressed for time due to a pending deadline, may opt for a less time and effort-consuming solution, albeit an insecure one.

These few and non-exhaustive examples show how psychosocial risks affect the users of Information Systems and consequently, Information Security. Irrespective of the level of security incorporated in systems and policies, the responsibility for Information Security largely lies with the end-user who has already been established as the weak link in the Information Security chain. When the user's abilities and will to protect the information he/she handles have been reduced by psychosocial factors, this information will inevitably be at peril. Hence, even though the user will always be expected to comply with policy requirements, every effort must be made to ensure that he/she is not hindered by psychosocial factors in doing so.

5. Proposed methods of assessment and mitigation – future work

By the discussion so far it should be clear that technological “add-ons” cannot solve all of the Information Security problems of an organisation upon deployment, as Information Security has to also address people issues and organisational aspects. To achieve this goal, all aspects of Information Systems and organisational issues must be designed or re-designed with Information Security as an element of the design process. Existing systems, applications and the complete information lifecycle must be re-examined, bearing in mind plausible Information Security principles.

There is little point in allowing psychosocial risks to go unchecked and then attempting to counteract their effects. This would be equivalent to treating the symptoms of a disease and not the disease itself. The best approach is to try and pro-actively diminish the psychosocial risks in the first place. To this end ILO provides detailed and up-to-date instructions (ILO, 1998; 2012). In order to be reduced, the psychosocial risks must first be identified and assessed. Following identification, the evaluation of psychosocial risks need not be obtained in absolute terms. It is more practical to obtain a base-line assessment of the situation at a given point in time and re-evaluate, after steps are taken towards psychosocial risk mitigation. Mitigation will take place by designing proper processes to this effect and incorporating appropriate controls. The virtuous cycle of perpetual re-assessment in order to evaluate the effectiveness of the controls has to be repeated periodically.

As this is both a tedious method to design and follow and expensive in terms of resources, senior management commitment is of paramount importance. To obtain such a commitment may be easier said than done, as described by Gagné et al. (2008,

p.73): *"all other IT activities are perceived more as enabling the business to do their work, where security is the one group that is perceived as the opposite".*

The assessment can take place using two methods: surveillance and questionnaires (Dollard, 2007). Surveillance relies on obtaining statistical data from sources like the Human Resources and Health departments of an organisation regarding personnel absences, complaints, decreased departmental efficiency, common ailments etc. Questionnaires can be based on 5-point balanced Likert scale structures (Likert, 1974) with gradations from "Not at all stressful" to "Extremely stressful" or "Very happy" to "Very unhappy" depending on the question subject. Also depending on the question subject, other forms of questionnaires may be used (Friedman and Amoo, 1999). The questionnaires having the capacity for much more accurate targeting of the effect of psychosocial risks on the security of Information Systems, they would be preferable to any other method of assessment that, nevertheless, can still be used to complement the questionnaire-based survey results and/or guide questionnaire design. This will be one of the topics of further research in this field.

A detailed examination of psychosocial risk mitigation being beyond the scope of this paper, future research in this area will be based on (among other sources) the work of Greitzer et al. (2010; 2010a; 2011) on combining psychosocial data with traditional cyber-security data and modelling towards insider-threat mitigation; on the work of Da Veiga and Eloff (2010) for Information Security culture assessment; on the writings of Vyhmeister et al. (2006) for risk assessment with respect to the implementation of information and communication systems; on Trompeter and Eloff (2001) for the implementation of socio-ethical controls in Information Security and on the works of Carlotto (2010) and Cifre et al. (2004) that deal with information technology-induced psychosocial risks and tools for their assessment.

6. Conclusions

In this paper, two existing research areas, that of psychosocial risk identification and management and that of Information Security, both well-researched in their own right, are brought together. Combining the two areas in research may bring us closer to an answer to the question of why Information Security fails when all prescribed measures and controls are in place and active. It may help us better understand the specificities of the effects of human nature on Information Security and in doing so, ameliorate the general environment in which humans are called upon to function in a secure manner. It may also help set a new paradigm on what constitutes a "reasonable request" from human operators of an information system when they are asked to uphold Information Security. Under this light and through a virtuous cycle of survey and re-assessment using specially constructed questionnaires, the real effect of psychosocial risks on Information Security will be established.

7. References

Brun, J.-P. 2003. *La Santé Psychologique au Travail... de la Définition du Problème aux Solutions*, Québec: Université Laval/IRSST, ISBN: 2-9807808-2-0

Carlotto, M. S. 2010. Fatores de risco do tecnoestresse em trabalhadores que utilizam tecnologias de informação e comunicação. *Estud. psicol. (Natal).* **15**(3) 319-324. Available on-line from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-294X2010000300012&lng=en&nrm=iso. Last access: 20.2.2012

Cifre, E., Salanova, M., Martínez-Pérez, M.D., Martínez, I., Llorens, S., and Grau, R. 2004. Developing a new tool to assess specific psychosocial risks among teleworkers: The RED-TT questionnaire. In: *Proceedings of the Third International Conference on Occupational Risk Prevention (ORP2004)*.

Cooper C. L. 1994. The Costs of Healthy Work Organizations in: Cooper, C. L. and Williams, S. (Ed.) *Creating Healthy Working Organizations*, p. 1-5, Chichester: John Wiley & Sons. Cited in Haubold B. 2008. *Les risques psychosociaux. Identifier, analyser, prévenir les risques humains*. Paris: Éditions d' Organisation Groupe Eyrolles

Cooper, C.L. Liukkonen, P., and Cartwright, S. 1997. *Stress Prevention in the Workplace: Assessing the Costs and Benefits for Organisations*. Dublin, Ireland: European Foundation for the Improvement of Living and Working Conditions. ISBN: 978-9282765036

Cox, T. 1993. *Health & Safety Executive Contract Research Report No 61/1993. Stress research and stress management: Putting theory to work*. UK:HSE Books. ISBN: 0717606848

Cox, T., Griffiths, A. and Randall, R. 2003. A Risk Management Approach to the Prevention of Work Stress. In: Schabracq, M., Winnubst, J. and Cooper, C. (Ed.) *The Handbook of Work and Health Psychology,* Ch. 10, p.191-206, Chichester: John Wiley & Sons, Ltd., ISBN: 9780470013403

Cox, T. and Griffiths, A., 2003a. Commentary III: Monitoring the changing organization of work: A commentary. *Sozial- und Präventivmedizin / Social and Preventive Medicine.* **48** 354-355

Da Veiga, A. and Eloff, J. H .P., 2010. A Framework and assessment instrument for Information Security Culture. *Computers & Security*. **29**(2) 196-207

EASHW - European Agency for Health and Safety at Work, 2002. *European Week 2002: Preventing psychosocial risks at work*. Website. http://ew2002.osha.europa.eu/. Cited in Leka, S. and Cox, T. (Ed.) 2008. The European Framework for Psychosocial Risk Management: PRIMA-EF, Nottingham: I-WHO Publications, ISBN: 978-0-9554365-2-9

EASHW - European Agency for Health and Safety at Work, 2007. *Expert forecast on emerging psychosocial risks related to occupational safety and health,* Luxembourg: Office for Official Publications of the European Communities. Cited in Leka, S. and Cox, T. (Ed.) 2008. The European Framework for Psychosocial Risk Management: PRIMA-EF, Nottingham: I-WHO Publications, ISBN: 978-0-9554365-2-9

Frangopoulos, E. D., 2007. *Social Engineering and the ISO/IEC 17799:2005 Security Standard: A Study on Effectiveness*, MSc Dissertation, University of South Africa.

Frangopoulos, E. D., Eloff, M. M. and Venter, L. M., 2008. Social aspects of Information Security. In: *Peer-reviewed Proceedings of the ISSA 2008 Innovative Minds Conference*. ISBN 978-1-86854-693-0.

Frangopoulos, E. D., Eloff, M. M. and Venter, L. M., 2010. Psychological Considerations in Social Engineering – The Ψ-Wall as defense. *IADIS International Journal on Computer Science and Information Systems.* **5**(2) 1-20. ISSN: 1646-3692.

Friedman, H. H. and Amoo, T. 1999. Rating the Rating Scales. *Journal of Marketing Management.* **9**(3) 114-123

Gagné, A., Muldner, K. and Beznosovet K. 2008. Identifying Difference between Security and other IT Professionals: a Qualitative Analysis. In: *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008).* 69-79

Greitzer, F. L., Noonan, C. F., Kangas, L. J. and Dalton, A. C. 2010. *Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats – PNNL 19665*. Available on-line from: http://www.pnl.gov/main/publications/external/technical_reports/PNNL-19665.pdf. Last access: 24.2.2012

Greitzer, F. L. and Frincke, D. A. 2010a. Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. In: Probst, C. W., Hunker, J., Gollmann, D. and Bishop, M., (Ed.) 2010. *Insider Threats in Cyber Security.* New York: Springer. ISBN: 978-1-4419-7133-3

Greitzer, F. L. and Hohimer, R. E. 2011. Modeling Human Behavior to Anticipate Insider Attacks. *Journal of Strategic Security*. **IV**(2) 25-48

Haubold B. 2008. *Les risques psychosociaux. Identifier, analyser, prévenir les risques humains*. Paris: Éditions d' Organisation Groupe Eyrolles, ISBN: 978-2-212-54240-0.

Heskett, J. L., Sasser, W. E. and Schlesinger, L. A. 1997. *The Service Profit Chain: How Leading Companies Link Profit and Growth to Loyalty Satisfaction, and Value*. New York: Free Press. Cited in Haubold B. 2008. *Les risques psychosociaux. Identifier, analyser, prévenir les risques humains*. Paris: Éditions d' Organisation Groupe Eyrolles

ILO – International Labour Organisation, 1986. *Psychosocial factors at work: Recognition and control. Occupational Safety and Health Series no: 56*, Geneva: International Labour Office, ISBN: 92-2-105411-X

ILO – International Labour Organisation, 1998. *Technical and ethical guidelines for workers' health surveillance. Occupational Safety and Health Series no: 72*, Geneva: International Labour Office, ISBN: 92-2-110828-7

ILO – International Labour Organisation, 2012. *Stress prevention at work checkpoints: Practical improvements for stress prevention in the workplace*, Geneva: International Labour Office, ISBN: 978-92-2-125637-3

Larson, W. J., Kirkpatrick, D. H., Sellers, J., Thomas, L. D. and Verma, D. (Ed.) 2009. *Applied Space Systems Engineering*, McGraw Hill, ISBN: 978-0073408866

Likert, R. 1974. The Method of Constructing an Attitude Scale. In: Maranell, G. M., (Ed.) 1974. *Scaling: A Sourcebook of Behavioral Scientist,* Ch. 19, 233-243, Chicago, IL: Aldine Publishing Company, ISBN: 978-0-202-36175-8

Leka, S. and Cox, T. (Ed.) 2008. *The European Framework for Psychosocial Risk Management: PRIMA-EF,* Nottingham: I-WHO Publications, ISBN: 978-0-9554365-2-9

Mathieu, J. E and Zajac, D. M. 1990. A Review and Meta-Analysis of the Antecedents, Correlates and Consequences of Organizational Commitment. *Psychological Bulletin*. **108**(2) 171-194. Cited in Haubold B. 2008. *Les risques psychosociaux. Identifier, analyser, prévenir les risques humains*. Paris: Éditions d' Organisation Groupe Eyrolles

Michie, S. 2002. Causes and Management of Stress at Work. *Occupational Environmental Medicine.* **59** 67–72

Probst, T. M., Gold, D. and Caborn, J. 2008. A Preliminary Evaluation of SOLVE: Addressing Psychosocial Problems at Work. *Journal of Occupational Health Psychology*. **13**(1) 32–42

Schneider, B., Hanges, P. J., Smith, D. B. and Salvaggio, A. N. 2003. Which Comes First: Employee Attitudes or Organizational, Financial and Market Performance? *Journal of Applied Psychology.* **88**(5) 836-851. Cited in Haubold B. 2008. *Les risques psychosociaux. Identifier, analyser, prévenir les risques humains*. Paris: Éditions d' Organisation Groupe Eyrolles

Schneier, B. 2004. *Secrets and Lies: Digital Security in a Networked World,* New York: John Wiley & Sons, Inc., ISBN: 978-0471453802

Spector, P. E. 1997. *Job Satisfaction: Application, Assessment, Causes, and Consequences.* Thousand Oaks: Sage Publications, Inc., p. 104. Cited in Haubold B. 2008. *Les risques psychosociaux. Identifier, analyser, prévenir les risques humains*. Paris: Éditions d' Organisation Groupe Eyrolles

Trompeter, C. M. and Eloff, J. H. P., 2001. A Framework for the Implementation of Socio-ethical Controls in Information Security. *Computers & Security.* **20**(5) 384-391

Vandenberg, R. J., Richardson, H. A. and Eastman L. J. 1999. The Impact of High Involvement Work Processes on Organizational Effectiveness: a Second Order Latent Variable Approach. *Group and Organization Management*. **24**(3) 300-339. Cited in Haubold B. 2008. *Les risques psychosociaux. Identifier, analyser, prévenir les risques humains*. Paris: Éditions d' Organisation Groupe Eyrolles

VERIZON Data Breach Investigation Report, 2009. Available on-line from: http://www.verizonbusiness.com/resources/executivebriefs/eb_2009_DBIR_snapshot_en_xg.pdf. Last access: 20.2.2012

VERIZON Data Breach Investigation Report, 2010. Available on-line from: http://www.verizonbusiness.com/resources/executivesummaries/es_2010-data-breach-report_en_xg.pdf. Last access: 20.2.2012

VERIZON Data Breach Investigation Report, 2011. Available on-line from: http://www.verizonbusiness.com/resouces/executivesummary/es_2011-data-breach-investigations-report_en_xg.pdf. Last access: 20.2.2012

Vyhmeister, R., Mondelo, P. R. and Novella, M. 2006. Towards a Model for Assessing Workers' Risks Resulting from the Implementation of Information and Communication Systems and Technologies. *Human Factors and Ergonomics in Manufacturing & Service Industries.* **16**(1) 39–59

Webster, S., Buckley, P. and Rose I, 2007. *Psychosocial Working Conditions in Britain in 2007*, Health & Safety Executive (HSE). Available on-line from: http://www.hse.gov.uk/statistics/pdf/pwc2007.pdf. Last access: 19.2.2012