Małgorzata Sidor-Rządkowska

Warsaw University of Technology

m.sidor.rzadkowska@pw.edu.pl

ORCID ID: orcid.org/0000-0003-3826-9382

JOURNAL OF MODERN SCIENCE
TOM 2/49/2022
www.jomswsge.com

DOI: https://doi.org/10.13166/jms/156776

HUMAN – THE WEAKEST OR THE STRONGEST LINK? THE ROLE OF ORGANISATIONAL CULTURE IN ENSURING CYBER SECURITY OF REMOTE WORK

Abstract

Specialists dealing with cyber security of organisations often cite the saying that a chain is only as strong as the weakest link in it. Experts alert that human error is the cause of more than half of the events in which corporate data has been lost. This issue becomes crucial in the times of widespread remote work. Since many professional duties have been performed recently at home or 'café' environment, organisations have been exposed to numerous threats, financial and image losses.

The aim of the article is to analyse these threats and to discuss the role of organisational culture in creating working environment ensuring cyber security.

Material and methods:

This paper is based on literature review. The starting point is the presentation of cyber security threats related to individual forms of remote work, such as work on company computer equipment outside the employer's premises, work on private computer equipment and work on computer equipment provided by a coworking centre.

Results:

The result of the research is the indication that in the remote work environment, activities aimed at strengthening cyber security should be undertaken on all indicted by Edgar Schein levels of organisational culture.

Conclusions:
Eventually, the article will indicate actions to be taken at each of these levels in order to foster employees' behaviour aimed at increasing cyber security.

Keywords: *remote work, cyber security, organisational culture, training policy*

Introduction

Increasing popularity of remote work since March 2020 resulted in many complex consequences. These have been subject to numerous in-depth analyses focused on revealing the complexity of remote work determinants from the employee's, employer's and society's point of view.

One of the key challenges connected with this form of work is ensuring security of company data. Working from home or in the 'cafe' environment poses many threats which may lead to severe financial and image losses.

Since the first months of the COVID-19 outbreak, reports have been multiplying showing the negative impact of this form of performing professional duties on the cyber security of organisations. It is commonly emphasised that remote work was forced by the epidemic situation and implemented without proper preparation. Many IT professionals (HP Wolf Security Report, 2021) admit they feel pressure to 'ensure business continuity at the expense of security. 83% of IT professionals surveyed by HP Wolf Security expressed the view that remote working is a 'ticking time bomb' when it comes to digital threats.

Very costly measures are taken in order to defuse this bomb. Therefore, huge investments are made in sophisticated security measures, and the salaries of highly skilled cyber security specialists are record-breaking. However, even the most modern sophisticated tools prove ineffective since 67% of employees admit to using the same password to log in to different accounts, and a significant number of the remaining employees write down new passwords on pieces of paper stuck near their computers (Wychowanski, Vecto 2021, p.15).

Stories of this type could be multiplied. One may also describe various everyday practices. These involve children using parents' work computers, leaving a laptop open for a moment on a café table – when observing these habits or behaviour of many people one may consider these practices as natural. Specialists alarm: human carelessness is the most common cause of data loss. It's time to draw conclusions and focus on creating a cyber-secure organisational culture as one of the company's priorities.

Forms of remote work and security of company data

When implementing remote work, organisations need to provide those working remotely with appropriate equipment. In practice, it is usually executed in one of the following forms:

a) Working on company computer outside the employer's premises;
b) Working on private computer;
c) Working on computer equipment provided by a coworking centre.

Let's try to consider each of these situations.

Re. a) From the data security point of view working on company computer hardware seems to be an optimal solution. However, many organisations are unable to equip each employee with a portable computer due to huge costs. Examples of significant limitations have been reported in numerous documents. Here is one such example: 'The five audited regional branches of KRUS (Agricultural Social Insurance Fund) as of the date of the COVID-19 outbreak had a total of only 77 portable computers for 1400 employees, of which the Koszalin and Łódź branches had three and five laptops respectively (for 163 and 467 employees respectively). Due to the insufficient provision of computer equipment only 6% of employees were able to work remotely. For more than a year of the COVID-19 outbreak, this condition did not improve' (NIK Report 2021).

Equipment availability is usually much better in successful commercial organisations. However, another problem must be mentioned here, that is access to company equipment by unauthorized people, such as household members and children in particular. The research conducted during *the school lockdown* period shows that most of the respondents shared their company laptop with a child who used it to learn remotely.

Re. b) Working on private computer equipment involves an even higher level of threats to information security. These devices are usually devoid of most of the safeguards used in business computers. Accounts are often not protected by passwords, there are no up-to-date antivirus programs, etc. Transferring files between work and private computers is particularly dangerous; nearly half (46%) of remote workers admit to doing so (Kozlowski 2020).

Re. c) Many authors indicate (e.g. Wychowański 2021) that working on computer equipment provided by a coworking centre poses particularly significant challenges related to the security of corporate data. A coworking centre is a place where office space is made available to representatives of various organisations. Users of this space may happen to leave memory sticks or passwords to company accounts in coworking computers, fail to log out from company e-mail box. These acts of negligence violate elementary rules of cyber security.

In addition to the signalised risks associated with remote work, there is one more often ignored problem. As noted by Piotr Wróbel and Tomasz Stefaniuk (2021, pp. 108-109), private smartphones and tablets are increasingly used for work related purposes. Most of these devices are not equipped with any security features to prevent loss of corporate data.

Three levels of corporate culture

The brief overview of remote work presented in the previous section indicates that treating the issue of securing corporate data solely as the responsibility of specialists is a huge mistake. A holistic approach is needed, and this in practice involves taking actions aimed at building organisational culture conducive to cyber security. A review of definitions of the above mentioned concept exceeds the framework of the article, thus we are going to focus on Edgar Schein's classic model. According to this model, there are three levels of organisational culture: the level of assumptions, the level of norms and values, and the level of artifacts. Assumptions reflect the deepest beliefs related to the nature of human beings and the world around them that underlie how a company operates. They are generally difficult to identify – as Edgar Schein emphasised, they are the invisible and unconscious level, but they exert a tremendous influence on all aspects of an organisation's operations. The second level, in turn, partially visible and conscious, is the level of norms and values. They can be both formal (e.g., work regulations) and informal, expressed as orders or prohibitions, only declared or both declared and applied. The visible and executed level of organisational culture is the third level – these are artifacts manifested primarily in the behaviour of employees. All these three levels should be internally consistent, otherwise the company will fall into a kind of 'cultural drift'.

Building a cyber-security-friendly organisational culture should start with a review of cultural assumptions. By no means is it an easy task. The researcher who has been combining her academic work with consulting activities in companies of various industries and sizes, argues that it requires at least several workshop meetings. During these meetings, participants are expected to identify the widespread, significant, yet hidden beliefs that affect information security. At the beginning of such discussion, one may, for instance, ask the participants to 'warm up' by filling out the form shown in the picture below.

Figure 1. Sample questions exploring cultural assumptions about information security.

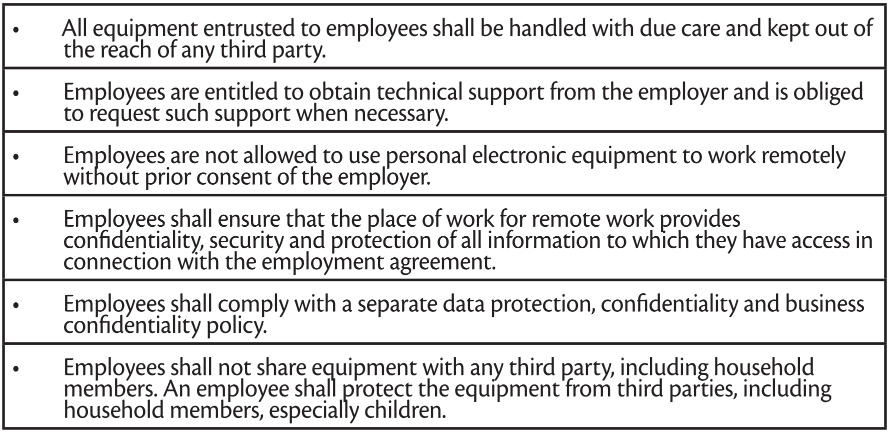
Evaluate the extent to which the following beliefs are prevalent in your company by circling the appropriate answer in each case:

It is believed in my company that information security is the sole responsibility of the IT department:				
Definitely	**Rather**	**Hard to**	**Rather**	**Definitely**
no	no	say	yes	yes
It is believed in my company that information security is the responsibility of every employee:				
Definitely	**Rather**	**Hard to**	**Rather**	**Definitely**
no	no	say	yes	yes
It is believed in my company that creating procedures is pointless, and they will be worked out in action:				
Definitely	**Rather**	**Hard to**	**Rather**	**Definitely**
no	no	say	yes	yes
It is believed in my company that employees have the skills to operate equipment similar to the job, training is not needed:				
Definitely	**Rather**	**Hard to**	**Rather**	**Definitely**
no	no	say	yes	yes

Source: own study—based on the researcher's literature review

These are – one should emphasise once more – sample questions, which may become a starting point for a discussion focused on identifying cultural assumptions in the area of company cyber security. Norms and values are easier to identify; as in the previous case, such an analysis should be accompanied by the question – to what extent do these elements serve the security of company data? Should the answer to this question be unsatisfactory, corrective action needs to be taken by introducing appropriate provisions into the company's rules and regulations. These may take the form of the illustration presented below.

Figure 2. Example of remote working regulations (excerpt):



- All equipment entrusted to employees shall be handled with due care and kept out of the reach of any third party.
- Employees are entitled to obtain technical support from the employer and is obliged to request such support when necessary.
- Employees are not allowed to use personal electronic equipment to work remotely without prior consent of the employer.
- Employees shall ensure that the place of work for remote work provides confidentiality, security and protection of all information to which they have access in connection with the employment agreement.
- Employees shall comply with a separate data protection, confidentiality and business confidentiality policy.
- Employees shall not share equipment with any third party, including household members. An employee shall protect the equipment from third parties, including household members, especially children.

Source: P. Wróbel, T. Stefaniuk, Implementation of Remote Work in organisations. People, Processes, Technologies, Security, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2021, p. 137.

However, it should be strongly emphasised that all provisions in the regulations will become a valuable element of the organisational culture provided they are not only declared but also observed. Is it really so? One may learn more by analysing the third level of organisational culture, which manifests itself in employee behaviour. A positive example could be, for example, the widespread participation of employees in training on cyber security and the application of the knowledge gained from these training sessions into daily practice.

Building pro-development organisational culture

It is the employee who is or at least should be responsible for their own professional development. One may argue that starting a job in a modern organisation has become in a way similar to taking up education. In view of the dynamic transformations occurring around the world, the need for constant improvement of one's competences is obvious. The employee's responsibility for their own professional development does not exclude the responsibility of the organisation. Employers are becoming increasingly aware of the importance of creating environment where employees' competences are developing faster than the changes occurring in the environment. Only then will competitive advantage be achieved and maintained. Although modern companies withdraw from designing traditionally perceived career paths calculated for a dozen or more years, they still need to make efforts to increase the potential of the people employed in the organisation. It is vital to align the individual aspirations of employees to the company goals.

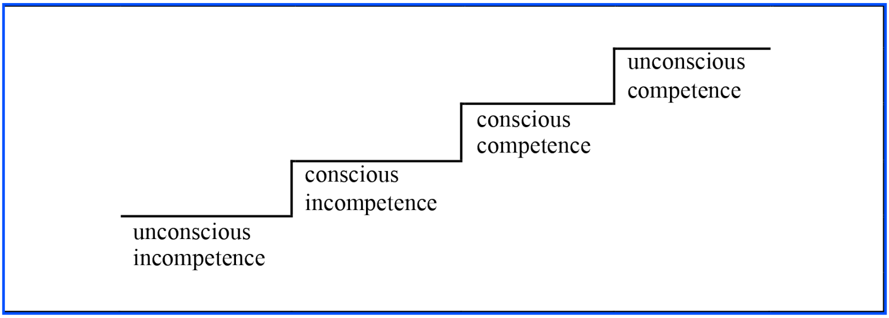
The above-mentioned statements have become increasingly significant in relation to the development activities aimed at increasing knowledge and skills concerning cyber security. In fact, it is difficult to identify another area where funds invested in employee development will protect the company from incurring huge financial and image costs.

A prerequisite for creating a pro-development organisational culture is first of all breaking with the still prevailing conviction that in human life there is a 'time to learn' and a 'time to work'. According to this view, at certain age one should devote oneself exclusively to professional activities and family duties, leaving the acquisition of new qualifications to young people. However, this approach is totally unacceptable these days and, in relation to the data security issues, may prove to be extremely irresponsible. The times when people could rely throughout their working lives on the knowledge they gained at school or university are long gone. Contemporary employees must recognise that throughout the entire period of their employment they will need to continuously improve their knowledge, even if they only wish to keep their current position. In view of the dynamic changes happening in the surrounding environment, joining a modern company becomes tantamount to starting education. This imposes certain obligations on the organisation. Therefore, both company's management and, in particular, the training department need to focus on creating pro-development company culture. All people employed in such organisation participate in the process of continuous expansion of knowledge. Moreover, the obligation to constantly improve one's qualifications is recognised as something obvious. Effective development policy must involve all employees, regardless of their age or length of service. Thus, the content, forms and methods of individual development activities must embrace the specific needs and skills of each employee.

At the start of development activities one should embrace the following statement: In the process of development 'there is a transition from unconscious incompetence *(I don't know that I can't)* through conscious incompetence *(I know that I can't)* and conscious competence *(I know that I can)* up to unconscious competence *(I just do)*, i.e. to a state when a person performs a task in a manner adequate to the situation, even though they do not fully engage their attention to perform it' (Kossowska , Soltysinska 2002, p. 86).

This rule is illustrated in the diagram below.

Figure 3. Competence ladder



Source: (Rae 2003, p.81)

Reaching the highest of these levels, i.e., the state in which an employee effectively performs their tasks without even being aware of it, is only seemingly the most desirable situation, since 'unconscious competence can easily turn into unconscious incompetence again. At the same time, one must recognise the fact that in case of numerous competences, automatic performance – even on very high level – does not indicate that one has reached the maximum of their potential. On the contrary, in order to reach the highest level, sometimes we need to switch off automatism. This is one of the vital elements of learning to drive a car in a skid – first, we need to turn off automatic reactions in order to learn non-intuitive but effective behaviour'(Filipowicz 2019, p. 54).

This metaphor seems to be fairly accurate – learning cyber security principles in the remote working environment may be compared to learning to drive a car in a skid.

Training policy — basis for creating a pro-developmental organisational culture

Training policy is fundamental in the proper formation of a pro-development organisational culture. The basic forms of developing this policy in the area of cyber security of remote working include:

- Traditional training – the main objective here is to provide employees with cyber security competences relevant to their jobs and to equip them with the skills to apply the acquired knowledge in practice. Such training can take both onsite and offsite forms. However, each of them has its own advantages and limitations. They need to be thoroughly analysed and adjusted to the external and internal circumstances of a particular organisation. One should remember that each training should include three aspects: educational, motivational and integrative (Sidor-Rządkowska 2020, pp.142-147).
- Group discussions – may be a part of training programme or a separate meeting set for several people persons, during which the participants share their experiences related to data security threats and ways of dealing with them. The communication here is multidirectional; the participants take turns leading the meeting.
- Instructional videos of various kinds – the advantage here is that the content can be used anywhere and anytime; the disadvantage is lack of opportunity for direct interaction with other employees.

- Video games – their advantage is an attractive form as they combine elements of learning and entertainment. On the other hand, though, they are usually characterised by a certain degree of triumph of form over substance; they do not provide structured knowledge on information security, but they definitely stimulate the acquisition of such knowledge.
- Manuals, handbooks, newsletters, etc.—they enable one to fully present organisation's key developments. They may be available in paper or electronic form – the latter allows the content to be updated quickly. The problem, however, is getting employees to read them regularly.

Adult learning is characterised by the focus on the practical value of the acquired knowledge. All attempts to change this attitude are both ineffective and unjustified. The management of a company should be committed to ensuring that all content provided within the framework of activities defined collectively as 'training policy' find their tangible reflection in the workplaces. The practical implementation of this principle requires many efforts, though. Special mechanisms must be developed to enable all training content to be translated into the daily performance of routine duties. The employee cannot be left alone in this. Moreover, when developing training programmes focus should be given to taking maximum advantage of the practical experience and pragmatic attitude of participants and therefor create environment where attention to the perception of cyber security principles becomes an internal need.

Conclusions

Ensuring the cyber security of remote working is an issue that organisations of all industries and sizes are straggling with therefore they focus on improving their tools and operating procedures. However, one should remember that implementing the most costly tools and procedures will not guarantee they will be properly followed. Thus, more attention should be given to the organisational culture as it is the glue and driving force of any company. It is worth conducting further research into how to create a cyber secure remote working environment. In such an environment, each employee has both the knowledge, skills and attitude aimed at ensuring the security of company data. While conducting the research one should recognise that 'humans are a vector for attacks not because they are a vulnerability in the system, but because their actions are less predictable than those of the system. This represents a risk, but at the same time is the greatest value of their work. (…) Therefore, a human being in an IT system should be seen as requiring special support because they are crucial to the processes, and not because of their problematic nature' (Surdyka 2021, p.55). It is the organisational culture that determines whether the human being becomes the weakest or the strongest link of the company's cyber security.

References

Ahmad, A., Maynard, S.B., Park, S. (2012), *Information security strategies: Towards anorganizational multi strategy perspective*, 25 (2). Journal of Intelligent Manufacturing.

Albrechtsen, E., Hovden, J. (2010). *Improving information security awareness and behavior. through dialogue participation, and collective reflection. An intervention study*, 29(4):432-445. Journal of Computers and Security.

Alexei, Arina, Alexei, Anatolie (2021). *Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning*. 10 (3), 128-133. International Journal of Scientific & Technology Research.

Ali, R. (2021). *Looking to the future of the cyber security landscape*, 2021 (3), 8-10. Network Security.

Allen, T.D., Golden, T.D., Shockley, K.M. (2015), *How Effective is Telecommuting? Assessing the Status of Our Scientific Findings*, 16 (2). Psychological Science in the Public Interest.

Bendkowski, J. (2018), *Coworking – nowa forma pracy w gospodarce cyfrowej*, 124. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie.

Borkovich, D.J., Skovira, R.J. (2020), *Working from home: Cybersecurity in the age of covid-19*, 21 (4), 234-246, 2020. Issues in Information Systems.

Bodsberg, L., Grøtan, T. O., Jaatun, M. G., Wærø, I. (2021). *HSE and Cyber Security in Remote Work, 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021, 1-8, doi: 10.1109/CyberSA52016.2021.9478249.

Chmura, J. (2017). *Forming the awareness of employees in the field of information security*, 8 (1). Journal of Positive Management.

Curran, K. (2021). *Cyber security and the remote workforce*, 2020 (6), 11-12. Computer Fraud & Security.

Eikenberry, K., Turmel, W. (2019). *Przywództwo na odległość. Jak być skutecznym przywódcą zespołów rozproszonych*. Poznań: Dom Wydawniczy Rebis.

Filipowicz G. (2019). *Zarządzanie kompetencjami. Perspektywa firmowa i osobista*. Wolters Kluwer, Warszawa.

Gach, D. (2018), *Kształtowanie elementów kultury organizacyjnej zorientowanych na zachowanie bezpieczeństwa informacyjnego*, 4, 157-169. Bezpieczeństwo. Teoria i praktyka.

HP Wolf Security Threat Insights Report 1H 2021, https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-1h-2021/ (Access, June 2022).

Hutchins, S., Britt, S. (2020). *Cybersecurity Policies for Remote Work*, 67 (9), 10-12. Risk Management.

Jabłoński, M., Mielus, M. (2010). *Zagrożenia bezpieczeństwa informacji w organizacji Gospodarczej*, in. M. Kwieciński (ed.) *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*. Kraków: Oficyna Wydawnicza AFM.

Kossowska, M., Sołtysińska, I. (2002). *Szkolenie pracowników a rozwój organizacji*. Oficyna Ekonomiczna, Kraków.

Kurek, M. (ed. 2021), *Barometr cyberbezpieczeństwa. COVID-19 przyspiesza cyfryzację firm*, raport KPMG. Organizacja pracy zdalnej w wybranych podmiotach wykonujących zadania publicznew związku z ogłoszeniem stanu epidemii. Informacja o wynikach kontroli NIK, wrzesień 2021.

Rae, L. (1999). *Planowanie i projektowanie szkoleń*, translated by A. Hędrzak. Dom Wydawniczy ABC, Warszawa.

Rae, L. (2003). *Planning and Designing Training Sessions*. Oficyna Ekonomiczna, Kraków.

Sabin, J. (2021), *The future of security in a remote-work environment*, 2021 (10), 15-17, Network Security.

Schein, E.H. (2010). *Organizational Culture and Leadership*, Jossey-Bass A. Wiley Imprint San Francisco.

Schultz, E. (2005), *The human factor in security*, 24 (6). Computers and Security.

Sidor-Rządkowska, M. (2020). *Kompetencyjne systemy ocen pracowników. Przygotowanie, wdrażanie i integrowanie z innymi systemami ZZL*. Wolters Kluwer, Warszawa.

Sidor-Rządkowska, M. (2021). *Kształtowanie przestrzeni pracy. Praca w biurze, praca zdalna, coworking*. Warszawa: Wolters Kluwer.

Stefaniuk, T. (2020a), *Bezpieczeństwo informacji w świadczeniu pracy zdalnej*, in M. Kubiak (ed.) Prawne aspekty informacji chronionych. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego.

Stefaniuk, T. (2020b), *Training in shaping employee information security awareness*, 7 (3). Entrepreneurship and Sustainability Issues.

Weil, T., Murugesan, S. (2020). *IT Risk and Resilience—Cybersecurity Response to COVID-19*, 22 (3), 4-10. IT Professional.

Woźniak, J. (2021), *Współczesne monitorowanie pracy. Podstawy teoretyczne i metody Zastosowania*. Warszawa: Wolters Kluwer.

Wróbel, P. (2013), Zakres zastosowania wideokonferencji w organizacjach, 5. Ekonomika i Organizacja Przedsiębiorstwa

Wróbel, P. (2014). *Komunikacja elektroniczna: zagrożenia i ich skutki dla organizacji*. Sopot: Wydawnictwo Uniwersytetu Gdańskiego.

Wróbel, P. (2020), *Kompetencje sprawnego telepracownika*, in. H. Czubasiewicz (ed.), *Sukces organizacji w warunkach gospodarki cyfrowej. Zarządzanie zasobami ludzkimi*. Sopot: Wydawnictwo Uniwersytetu Gdańskiego.

Wróbel, P., Stefaniuk, T. (2021). *Implementation of Remote Work in organisations. People, Processes, Technologies, Security*. Wydawnictwo Uniwersytetu Gdańskiego.

Wychowański, J. (ed. 2021), *Cyberbezpieczeństwo w polskich firmach*, report Vecto.