INCENTIVIZING LOW-LEVEL ORGANIZATION MEMBERS BY INCREASING THEIR BEHAVIOUR FACTORS IS CRUCIAL FOR AN INNOVATIVE AND SECURE UP-TO-DATE WORKFORCE

A LITERATURE REVIEW ON DATA SECURITY AND SECURITY CULTURE IN DATA-GATHERING AND DATA-HANDLING ORGANIZATIONS

Krešimir Fileš, Phd candidate, MBA MHRES*

Abstract: In accordance with technological advancement and innovation in the contemporary digital business world, it has come to the Authors attention that technology focused protection and generally advancement is the “easy”, “temporary” and “fast” solution to growing digital security problems of modern data-gathering and data-processing organizations. In the Authors opinion, a socio-cultural change is needed as a foundation for these technological (technical) security

* Krešimir Fileš, Master of Business Arts in Marketing and Magister of Human Resources and Education Systems, is a PhD candidate of Organizational Sciences and Work Systems at the Faculty of Organizational Sciences, University of Maribor, Republic of Slovenia. His research interests include security culture and socio-cultural elements in organizations, adaptable and contemporary organizational structures, workflows and models in hybrid digital environment for data-gathering and data-handling organizations, cybersecurity, personal data protection and GDPR. files.kresimir@student.um.si kreso5344@gmail.com

measures. The said statement is gaining momentum in the scientific community, and therefore, the Author conducted a literature review as to further investigate. The problem primarily concerns the security culture of an organization which heavily relies on human factors, precisely the BEHAVIOUR factors. By taking in the human factor, combined with the knowledge factor and technical factor concerning data handling and defense against digital threats - this research tends to prove as to how, in the post COVID digital world, it is not enough for an organization to just implement technically, but it also needs to implement socio-culturally.

Keywords: culture, data, organization, behaviour factors, security

Introduction and problem definition

By researching multiple articles and scientific studies on the field of modern organizational structures and workflows suitable for the contemporary hybrid business world, which mainly refers to data-gathering and handling organizations, the Author noticed that the focus was generally of structural and technological nature - as opposed to concerning itself with the issue of employee BEHAVIOUR and CULTURE. In short, previous research did not give a substantial amount of attention to the problem of security culture which can be incentivized by increasing the BEHAVIOUR factors of data-gathering and handling employees.

Aside from the said problem, a need arises for a STRATEGIC CULTURE in terms of building a "sense" or a "feeling" of "belonging" that workers need to develop for their organization. The goal would ultimately be to connect employees to genuinely "care" for the organization they are working for. In the Authors opinion – this can be achieved by increasing the BEHAVIOUR factors of the said workforce.

In this literature review the Author showcased the culturally and socially oriented solutions to contemporary organization

problems of today, which heavily rely on BEHAVIOUR factors. These solutions come together with structurally and technologically oriented solutions to the problems of data-gathering and handling security issues. Although the structural and technological solutions are extremely important - it is the Authors aim to show that SECURITY CULTURE is the basis for such structural and technological solutions. The premise is that both are mandatory in a contemporary organization that tends to survive in the hybrid world, and SECURITY CULTURE should be seen as the foundation to all. The socio-cultural segment is mostly overlooked in today's business practice where resources are mostly spent on technology and structure – but not the socio-cultural elements and enhancing the workforce's BEHAVIOUR FACTORS.

According to Jenko A., Roblek M. (2016.): "Behaviour is the way one acts or conducts oneself, especially towards others (Oxford Dictionaries, 2016). We distinguish between individual and group behaviour. The behaviour of one individual has a strong impact on the behaviour of other individuals inside a group or organisation. Organisational behaviour is a field of study that investigates the impact that individuals, groups, and a structure have on the behaviour within organisations and it studies many factors that have an impact on how individuals and groups respond to and act in organisations and how organisations manage their environments. Under this name we therefore have an important group of psychological factors that influence other primary human factors. The main influence factors derived from the quoted HCSFs research articles and behaviour theory are: Motivation (personal and collective), Commitment, Responsibility, Trust, Empathy (understanding the needs of customers and interpersonal in a team), Expectation, Satisfaction (fulfilling personal needs and preferences), Satisficing (typical behaviour of decision makers), Propensity to take risk, Propensity to conflicts, Personal interest (principal-agent or agency theory), Knowledge withholding intentions, and Normal conformity."[1] Where: HCSF stands for Human Critical Success Factor; PHF stands for Primary Human Factor; CSF stands for Critical Success Factor.

[1] Jenko A., Roblek M. (2016.) A Primary Human Critical Success Factors Model for the ERP System Implementation, Organizacija 49

The modern organization of today is an organization of change – therefore an organization of projects. Constant progress and projects are needed to "keep afloat" in the business world. Structurally and process-oriented, where structure adapts to the processes. The efficiency of processes relies on human factors –BEHAVIOUR factors. In a data gathering and processing organizations (which the majority are today, eg. HR in any organization) there is also the data security issue. Aside from technical security measures, a security culture is needed that creates and supports a safe work environment.

Previous literature review and current research methodology

In table 1. a previous literature review is visible on the topic of social (BEHAVIOUR) factors and their impact on security culture of an organization.

Table 1. Previous literature review

	Authors	Papers	Year of earliest published paper	Central theme
1	Jenko and Roblek	1	2016.	Models for organizations
2	Turner and Miterev	3	2019.	Organization designs
3	Schraeder, S. Tears and H. Jordan	26	2004.	Organizational culture
4	Logan, Rollings, Clougherty Jones, Duncan and Toncheva	1	2020.	Annual CDO Survey
5	Fenn , Mesaglio , Olding	1	2018. (refreshed/updated version 2021.)	Culture Crush: Design Your Roadmap for a Culture of Innovation

Source: (Author)

Where CDO stands for Chief Data Officer.

Although the socio-behavioural and cultural segment is mentioned, most of the sources were mainly focused on structural changes to achieve organisational goals. Considering that both segments are important, the Author wishes to further explore more up to date papers and see the changes in prioritizing socio-behavioural and cultural segment as a foundation for structural changes within organisations.

In the review of previous literature it is also evident that, with the advancement of time, topics have become more and more socio-behaviourally and culturally oriented. In other words – the theme of culture (organization culture) becomes mentioned far more often as new papers are published regarding organisation models, designs, implementations and generally new technology. This is especially evident in the post-COVID hybrid business world which seems to have technologically and structurally jumped and the socio-cultural part was neglected.

According to Logan D., Rollings M., Clougherty Jones L., Duncan A., Toncheva A. (2020.) and the survey analysis they conducted - one of the key findings as to what a successful data and analytics program needs to strive for regarding CDO's is creating and encouraging culture change that emphasizes purpose and mission. This especially relates to collaborative working.

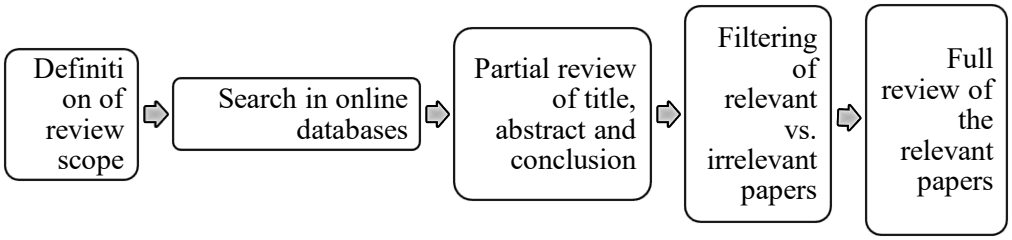
A literature review was conducted as shown in figure 1., in which the following databases were searched: Gartner, Web of Science and SAGE. The keywords used/combined were: Culture, behaviour, organization, people, IT, security, technology implementation, Cybersecurity, personal data. For easier navigation and narrower focus, the most relevant were presented and further researched and reviewed (as shown in table 2.).

The purpose was to find contemporary research papers that evolve around organization culture, culture shift to resolve technological implementation problems and increase data security. New technology presents a risk especially in the digital world concerning data gathering and processing organizations where a single mistake or negligence may cost millions. It is the Authors opinion that technical security measures need a socio-cultural foundation of organization members, feeling responsible and "caring" for their company, to fully utilize a safe work environment.

- Hypothesis that was tested and ultimately confirmed:

> By incentivizing low-level data gathering and handling organization members on being innovative in terms of data security we build and maintain a security culture that has the data security segment up to date.

Figure 1.: Research approach



Source: (Author)

In addition to the research approach, table 2. shows the results of the assessed and reviewed literature. Literature that was seen as eligible was in a span of 2021. – 2022. The aim was not only to see the difference between previous literature and present (now and then), but also the effect of COVID-19 on new ways of thinking in the scientific community. It is the creation of a new hybrid business world, in which culture, especially security culture needs a bigger role. It needs to be implemented and developed by organization leaders through BEHAVIOUR factors of organization members.

Table 2.: Results of the assessed and reviewed literature

Database	**Keywords**	**Total (total evaluated)**	**Total filtered relevant publications**
Gartner	Culture	1188 (80)	18
Web of Science	Cybersecurity	3195 (10)	1
Sage	Organization technology	26 (5)	1
SUM	Culture, cybersecurity, organization technology	4409 (95)	20
Total net hits			**20**

Source: (Author)

In the above given table, databases present the scientific databases searched. Keywords present filtered keywords that gave best results for the theme. Out of total results that showed, the bracketed number represents which were found relevant concerning mainly their title. After the titles were filtered, out of those selected another assessment occurred regarding the abstract and conclusion of the given papers. This was the final step as the selection was used to present a literature review of the finalist works (total net hits).

Findings and conclusion

Developing security culture as a foundation for further developments in data gathering and handling organizations – specifically by incentivizing low-level organization members BEHAVIOUR factors seems to be the way to digital business success according to Fenn J., Mesaglio M., Olding E. (2018.) from the previous literature review. In the mentioned paper, a culture of innovation is mentioned as a solution to the obstacles of digital business success:

> "The lack of an innovative culture is an obstacle to digital business success. This research provides a roadmap for CIOs to make their enterprises more creative and drive innovation levels higher. It is part of a set that helps CIOs design their innovation activities through a customizable framework…
>
> …Innovation leaders need to identify specific behavioural goals of a cultural change effort, as well as the current organizational context that shapes the choices…
>
> …Changing the culture involves recognizing that innovation is not always separate from day-to-day operations. Sometimes, it needs to be day to day…
>
> …Innovation leaders often need to effect change beyond their immediate teams. They need to work by influencing, encouraging and supporting other leaders in their innovation journeys…"[2]

[2] Fenn J., Mesaglio M., Olding E. (2018.) Culture Crush: Design Your Roadmap for a Culture of Innovation, Gartner

- Moreover, the authors continue to move on to BEHAVIOURAL and social dissection of the problem:

> "How work gets done and what gets rewarded today, for example: What are the dominant performance metrics? What behaviours and actions get people rewarded/promoted? What behaviours and actions get people punished?"[2]

The solutions (ideas and practices) this paper from 2018. (refreshed as of 2021.) offered to the problem of implementation and flexibility of organizations in an ever-changing digital world were continued and further developed in later works such as Struckman C., Sanchez Reina D., Gabrys E., Ramirez J. (2021.): The Culture PRISM: 5 Dimensions That Shape Culture.

Culture is clearly influenced by BEHAVIOUR FACTORS. Measuring and metrics to assess security culture should be conducted by evaluating the human factor – BEHAVIOUR factor. Listen to the low-level data gathering and handling employee; get him to innovate, incentivize him, make him feel he "belongs" to the organization and acknowledge his importance.

To fulfill all these tasks - it is of utmost importance to train executives and managers on creating a climate for this type of change. Their way of communicating and their general relationship with their subordinates becomes the focal point in executing these changes and developing security culture.

- According to Struckman C., Sanchez Reina D., Gabrys E., Ramirez J. (2021.):

> "Culture is often viewed as a barrier and hard to change, but it is also a source of strength: Culture helps employees know what is expected, accepted and respected."[3]

This is of critical importance as the hybrid business world is constantly changing world. By knowing what is expected,

[3] Struckman C., Sanchez Reina D., Gabrys E., Ramirez J. (2021.) The Culture PRISM: 5 Dimensions That Shape Culture, Gartner

accepted and respected – low-level data-gathering and processing employees have another layer of security aside from the technical and structural security measures. The Author would also argue that this layer is the foundation layer of data-gathering organization security in the digital world. Upon security culture further structural and technical security can reach its full potential. By "caring" for the organization and feeling responsible for their actions can the workers achieve a safe work environment. This can be measured and evaluated by their BEHAVIOUR factors. A happy, content, responsible workforce, which knows what is expected, accepted and respected can drive a flexible, resilient contemporary data-gathering organization to success.

This finding would confirm the given hypothesis.

- In further review, according to Judah S., Murray M. (2021.):

"Digital business transformation is disruptive, bringing with it both significant opportunities and risks. If data and analytics leaders and CDOs are to be successful, they must encourage a culture in which their teams understand and engage with risk, rather than try to avoid it…

…In most organizations, data and analytics teams have a poor risk-engaged culture, viewing risk as something to mitigate or avoid completely. As a result, data and analytics leaders can miss opportunities or accept too much poorly understood risk, which are both bad for business…

…Evaluate your data and analytics team's awareness, attitude and knowledge relating to information risk, and assess the potential or actual impact this culture has on achieving business outcomes…

…Establish a plan to improve the risk engaged culture in data and analytics teams, and use your existing governance framework to drive the change and transformation needed."[4]

[4] Judah S., Murray M. (2021.) Create a Risk-Engaged Culture in Your Data and Analytics Teams, Gartner

Which also goes hand in hand with the projected need to mandate a culture of organizational resilience to survive digital threats. A SECURITY CULTURE: "By 2025, 70% of CEOs will mandate a culture of organizational resilience to survive coinciding threats from COVID-19, cybercrime, severe weather events, civil unrest and political instabilities."[4]

It is clearly shown that culture and BEHAVIOUR factors will play a crucial role in the future of data driven business. Also, there is rarely a company that does not gather and process data. It could be argued that every company that possesses an HR or an accounting department has a data driven segment which handles sensitive data. In all these workflows, security culture must be present in order to maintain a safe work environment.

- Moreover, to the problem of awareness which is directly connected to cybersecurity (security culture) the following conclusion was made by Alsharif M., Mishra S., AlShehri M. (2022.):

> "There are different security vulnerabilities and security flaws in applications that interact over the internet. The overall results highlighted that the level of awareness related to cybersecurity issues (61%) had been achieved, which is an alarmingly low level that requires it to be increased to the maximum extent. The results show the lack of awareness of social engineering (37%), social media (35%), phishing (30%), passwords (30%), email usage (22%), antivirus (33%), and data protection (29%). This study found that the sample has a high lack of awareness about the top three vulnerabilities related to cybersecurity, and the major problem needs to be addressed and reduced through proper awareness and training…"[5]
>
> Where: the number of tested participants was n=333 and the percentage was calculated by category where the same participant may not be aware of multiple vulnerabilities (eg. 37% out of 333 participants show a lack of awareness of social engineering - some of those

[5] Alsharif M., Mishra S., AlShehri M. (2022.) Impact of Human Vulnerabilities on Cybersecurity, Computer Systems Science & Engineering 40(3)

> participants may also exhibit a lack of social media awareness).
>
> "… Another variable that showed a strong relationship was the issue of unsubscribing from emails after finishing work…
> …Hacking personal details of the companies and users can be done by the attackers using malicious codes and cyber-attacks, for which it is important to secure internal networks and communication channels. The human factor is the primary cause of security, and companies are not focusing on insider risks due to which they can suffer from the cyber-attacks and due to lack of awareness about cyber-security employees are not able to defend against cyber-threats and vulnerabilities. To encouraging compensation that helps the organization educate users. This step takes at least 9 to 10 months between phishing, gathering information, and creating appropriate training paths. Future work is required to conduct other comprehensive surveys among educational, governmental, medical, and industrial institutions to measure information security awareness among their employees and provide various statistical results to help them identify and address all weaknesses."[5]

Which simply dictates that for the most part – no security culture is present. Therefore, employees do not care if they unsubscribed their e-mail, if they have clicked on a malicious link and similar. If employees felt responsible and "cared" for the company, and if that kind of culture was created and developed through training and building relationships, the cyberthreats could be averted. This again would confirm the hypothesis given in chapter 3 on a more technical level.

Culture, the sum of unconscious, automatic success behaviours of individuals in the organization. From the brain's perspective, a "success behaviour" is any behaviour that is positively reinforced, and not just behaviours that lead to organizational success.

The Author would like to define SECURITY CULTURE as the sum of unconscious, automatic success behaviours of individuals in the organization. Behaviour that is positively reinforced when avoiding (or seeming to avoid) all possibility of data leakage and encourages risk evasion. Includes innovative thinking and

encourages ideas for securing organization data and averting data threats (external and internal). Is developed by increasing BEHAVIOUR factors of organization members. As the Author has shown – a more culture-oriented approach to contemporary organization survival in the hybrid business world is needed. Looking at the reviewed papers the Author can see that this theme is gaining more and more momentum as time passes on. It is evident that the scientific community, maybe under the influence of COVID-19 changes in business, is taking more interest in this topic than before.

Although the purpose of this literature review was to: show that by incentivizing low-level data gathering and handling organization members on being innovative in terms of data security we build and maintain a security culture that has the data security segment up to date; the Author cannot not acknowledge that the topic is becoming more and more popular as time passes.

- In this paper, the following hypothesis was confirmed:

> By incentivizing low-level data gathering and handling organization members on being innovative in terms of data security we build and maintain a security culture that has the data security segment up to date.

To conclude, all the technical security measures are immensely helpful in averting digital threats - but ultimately a modern organization must have a security culture built upon enhancing the BEHAVIOUR factors. Happy, content, "caring" and workers that feel a "belonging" to their organization will outperform an organization without the given qualities. With the growth of technology, digital threats also grow. To outmanoeuvre the threats and escape danger an organization cannot simply rely on technical security measures. The cyberthreats grow fast and therefore a sensitive, responsible and above all vigilant security culture must be always in place to create a safe work environment.

Literature:

1. Alsharif M., Mishra S., AlShehri M. (2022.) Impact of Human Vulnerabilities on Cybersecurity, Computer Systems Science & Engineering 40(3)
2. Fenn J., Mesaglio M., Olding E. (2018.; updated 2021.) Culture Crush: Design Your Roadmap for a Culture of Innovation, Gartner Inc.
3. Jenko A., Roblek M. (2016.) A Primary Human Critical Success Factors Model for the ERP System Implementation, Organizacija 49
4. Judah S., Murray M. (2021.) Create a Risk-Engaged Culture in Your Data and Analytics Teams, Gartner Inc.
5. Logan D., Rollings M. (2019.; updated 2022.) CDO Success Factors: Culture Hacks to Create a Data-Driven Enterprise, Gartner Inc.
6. Logan D., Rollings M., Clougherty Jones L., Duncan A., Toncheva A. (2020.) Fifth Annual CDO Survey, Gartner Inc.
7. Logan D., Rollings M., Duncan D. A., Idoine C., Clougherty Jones L., Subramanyam J., Heizenberg J., Davis M., Toncheva A. (2022.) CDO Agenda 2022: Pull Ahead By Focusing on Value, Talent and Culture
8. Schraeder M., Tears S. R., Jordan H. M. (2004.) Organizational culture in public sector organizations Promoting change through training and leading by example, Leadership & Organization Development Journal 26(6), 492-502
9. Struckman C., Sanchez Reina D., Gabrys E., Ramirez J. (2021.) The Culture PRISM: 5 Dimensions That Shape Culture, Gartner Inc.
10. Turner R., Miterev M. (2019.). The organizational Design of the Project-Based Organization, Project Management Journal 50(4), 487-498