Working from home during COVID-19 crisis: a cyber security culture assessment survey

Anna Georgiadou¹ · Spiros Mouzakitis¹ · Dimitris Askounis¹

Accepted: 4 February 2021 / Published online: 26 February 2021

© The Author(s), under exclusive licence to Springer Nature Limited part of Springer Nature 2021

Abstract

This paper aims to evaluate the cyber security culture readiness of organizations from different countries and business domains when teleworking became a necessity due to the COVID-19 crisis. We have designed a targeted questionnaire and conducted a web-based survey addressing employees while working from home during the COVID-19 spread over the globe. The questionnaire contained no more than 23 questions and was available for almost a month, from 7th April 2020 until 3rd May 2020. During that period, 264 participants from 13 European countries spent approximately 8 minutes to answer it. Gathered data were analyzed from different perspectives leading to evolutionary findings regarding information security readiness and resilience of both individuals and organizations. In this paper, results are being presented and discussed in detail while focusing on future scientific routes and research paths that need to be explored. It concludes on a number of cyber security recommendations addressing both the emerged vulnerabilities and the need for security culture evolution.

Keywords Cyber security culture · Assessment · COVID-19 pandemic · Remote working

---

✉ Anna Georgiadou
ageorgiadou@epu.ntua.gr

Spiros Mouzakitis
smouzakitis@epu.ntua.gr

Dimitris Askounis
askous@epu.ntua.gr

¹ Decision Support Systems Laboratory, National Technical University of Athens, Iroon Polytechniou 9, 15780 Zografou, Greece

Introduction

Coronavirus disease 2019, widely known as COVID-19, is an infectious disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) (Velavan and Meyer 2020). The disease was first identified in December 2019 in Wuhan, the capital of China's Hubei province (Hui, et al. 2020), and has since spread globally. In March 2020, the World Health Organization (WHO) declared the COVID-19 outbreak a pandemic (WHO Director-General's opening remarks at the media briefing on COVID-19 2020). Human casualties increase daily and cure is yet to be found. However, COVID-19 is much more than a health crisis.

During the first semester of its spread, infected civilizations realized its profound political, social and economic side-effects. People were advised to stay at home and, in most cases, forced to do so via a number of government mandates. Schools, shops, entertainment facilities and numerous other businesses temporarily closed as a counter measure to control the virus expansion, while remote working was encouraged in cases where the job nature allowed it. This normality disturbance caused a chain reaction to agriculture, manufacturing, retail, accommodation and food services, business and administrative activities and many other domains across a range of economic sectors. Affected businesses face catastrophic losses, which threaten their operations and solvency, while their workers are vulnerable to income loss and layoffs.

According to the International Labour Organization (ILO) Monitor, published on 7th April 2020, full or partial lockdown measures are affecting almost 2.7 billion workers, representing around 81% of the world's workforce (ILO Monitor:COVID-19 and the world of work. Second edition 2020). The COVID-19 crisis is expected to wipe out 6.7% of working hours globally in the second quarter of 2020—equivalent to 195 million full-time workers. As a result, losses across different income groups are estimated to exceed the effects of the 2008–2009 financial crisis.

Less affected businesses, and in some cases even benefitted by this unprecedented crisis, are the ones that have invested effort, time and budget on their digitalization. In other words, the ones that have significantly embedded information technology to their everyday activities allowing them to continue uninterruptedly their operations. These organizations, although in better terms compared to their technologically primitive rivals, face another COVID-19 side-effect not that apparent: the cyber-crime increase.

Cyberthreats are constantly evolving in order to take advantage of online behavior and trends. The COVID-19 outbreak is no exception. From the very beginning of the COVID-19 crisis, criminals have used the coronavirus to carry out social engineering attacks themed around the pandemic to distribute various malware packages. On March 9th 2020, a security researcher at Reason Labs, Shai Alfasi, has revealed that cybercriminals were using fake versions of decrease spread maps to obtain access to personal data stored in user's web browsers (credentials, credit card data, etc.) (COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report 2020). According to the UK National Fraud & Cyber

Security Centre, Coronavirus-related fraud reports increased by 400% in March 2020 (Coronavirus-related fraud reports increase by 400% in March 2020) while costing their victims over 800 thousand pounds in one month.

Based on Europol's Report (Pandemic profiteering: how criminals exploit the COVID-19 crisis [2020](#)), cybercriminals also seek to exploit an increasing number of attack vectors as a greater number of employers institute telework and allow connections to their organizations' systems. Attacks on critical infrastructures have already been reported, with the troubling example of the Brno University Hospital at Czech Republic, on March 12th 2020, which was forced to shut down its entire IT network, impacting also two of the hospital's other branches, the Children's Hospital and the Maternity Hospital.

Hospitals, medical centers and public institutions are being targeted by cybercriminals for ransomware attacks—since they are overwhelmed with the health crisis and cannot afford to be locked out of their systems, the criminals believe they are likely to pay the ransom. At the same time, thousands of new sites related to COVID-19 are created every day to carry out spam campaigns, phishing, spreading malware or to compromise Command and Control servers (Europol [2020](#); Interpol [2020](#); ENISA [2020](#)).

Cyber Security Centers and experts around the globe have issued recommendations and prevention tips to assist individuals to resist against cyber-crime and fraud. With an increasing number of countries encouraging citizens to stay, learn or work from home, focus on cyber security is more demanding than ever. The question that derives given the circumstances is: how the COVID-19 crisis has affected the cyber security culture of both individuals and organizations? Our initial hypothesis being that coronavirus pandemic caught the business world off guard and, since cyber security culture is only now starting to emerge as a term, could not be unaffected by this crisis.

This paper presents a survey for evaluating the cyber security culture side-effects due to COVID-19 pandemic while working from home. “[Methodology](#)” section presents a detailed methodology in an effort to develop a brief, targeted and comprehensible survey for the assessment of the cyber security readiness of organizations during the crisis with emphasis on employees' feelings, thoughts, perspective, individuality. In “[Considerations and Limitations](#)” section, we outline a number of considerations and limitations regarding the conducted survey. In “[Detailed Survey Results](#)” section, collected data are examined and analyzed under different prisms. A number of graphical representations and tables are being used to deliver survey results and, finally, highlight the key findings presented in “[Key Findings](#)” section. Finally, “[Conclusion and Future Work](#)” section concludes with the importance of our findings, the challenging scientific opportunities that arise from them and, most importantly, a number of critical cyber security culture recommendations which can prove to be of great assistance during this rather demanding period of time.

Fig. 1 Cyber security culture model

Fig. 2 Cyber security culture evaluation methodology

Methodology

Theory

Over the last year, we have designed and developed a cyber security culture framework for assessing the readiness of an organization with focus on human factor (Georgiadou et al. 2020c). It is based on a model which represents the key factors affecting and formulating the cyber security culture of an organization. This model clearly defines two levels, organizational and individual, each one divided into different dimensions, which, in turn, are consisted of different domains, with distinctive application areas and quantifiable indicators. Corresponding model is being presented in Fig. 1 reaching down to the dimension division but not expanding to the detailed domain level since such a detail is out of scope for this paper.

Suggested cyber security culture framework defines an evaluation methodology, presented in Fig. 2, with simple yet meaningful steps in order to assess each one of

the predefined security controls and gradually build an accurate representation of the security culture status of any living and evolving business structure.

Hereafter presented survey was designed based on the main principles and characteristics of this framework while using its core components and key elements to provide intelligence to the subject under consideration (Georgiadou et al. 2020b).

Steps

Designing the survey

Bearing in mind that present survey was meant to evaluate the cyber security culture side-effects during the COVID-19 crisis, a number of criteria needed to be met:

1. **Life-cycle:** Based on various social, psychological and humanitarian theories, the survey should be conducted while remote working was still applicable. In other words, while special legislation measures were still in place and prior to normality being brought back to our lives. This way it would attribute real life circumstances and avoid meeting with the displeasure of people asked to recall a recent painful past.
2. **Duration:** Being limited at home, for most of the people, proved to be more demanding than usual routine since they had to cope with business, family and household demands at the same time. As a result, time was more precious than ever and, for someone to participate to a survey without any obvious gain, it had to be brief and easily comprehensive querying no more than 5 to 10 min.
3. **Accessibility:** Since staying at home is the only credible defense armor against the virus, the survey needed to be digitalized and web-circulated allowing participation to individuals around the globe.
4. **Plainness:** The survey was targeting workers from numerous different business domains not necessarily familiar with technological and information security terms. Consequently, questions needed to be simple indirectly extracting the required answers. In many cases, help text was provided to further assist in understanding the question at hand.

Taking into consideration all of the above, a web-based questionnaire was created containing no more than 23 questions. Each question was founded on the cyber security culture model presented in the previous paragraph and aimed to get a generalized feedback. It has been hosted on an enterprise cloud solution and shared via a public link. Collected data are available via our enterprise cloud form (Georgiadou and Mouzakis 2020) and have been made available via a research data repository (Georgiadou et al. 2020a).

Validity testing

Having formulated a first version of the questionnaire, the next step was a validity testing in which around 20 people were asked to review and complete the survey.

This phase was conducted with a focus group consisted of a survey expert, experienced researchers and analysts, certified security and technology officers and simple workers with average technological knowledge. Its goal was to identify ambiguous questions or wording, unclear instructions, or other problems prior to widespread dissemination (Draugalis, Coons and Plaza 2008). The respondent debriefing and cognitive interviewing assisted in evaluating the clarity of the questions and the understanding of terms (Willis 2004). Think-aloud and verbal probing techniques (Fowler Jr and Fowler. 1995) were exploited to identify areas of possible misunderstanding. Taking into consideration input from this phase, we reached to a final version of the survey (Supplementary Appendix A) and the hosting cloud form used.

Sample selection

Specific survey was targeting workforce from countries affected by the coronavirus pandemic. Its goal was to identify the cyber security culture side-effects with special focus on European critical national infrastructures (CNI). Therefore, representatives from energy, transport, water, banking, financial market, healthcare and digital infrastructure were selected from different European countries (e.g., Cyprus, France, Germany, Greece, Italy, Romania, Spain) affected by the COVID-19 crisis. Such organizations, which needed to remain fully functional and limit operations impact to the minimum during this rather demanding period of time, require a deeper security culture. Consequently, monitoring and evaluating their status and locating possible cultural issues bears a special scientific interest.

Main study

A special invitation email (Supplementary Appendix B) was sent to the selected sample so as to ensure that data collection was limited to the specific target group. Making it widely available via a variety of communication channels, although feasible, was rejected after careful consideration by the authors. Results needed to be accurate, reliable and valid and, therefore, directly inviting corporations participating in a number of Horizon 2020 European Commission funded projects appeared to be a “safer” dissemination approach. Invitations were sent to representatives who were in turn asked to propagate the survey within their organization.

Presented survey was available for participation for 27 days, starting from 7th April 2020 and ending on 3rd May 2020. During that period, 264 *participants* visited the survey web form and completed the online questionnaire at around 8 min (average completion time). Around 90% of the participants were aged between 25 and 54 years old, while 84.46% had a higher educational degree (bachelor, master or doctorate). Representatives from different business domains provided feedback to our survey with three dominating sectors: *IT (Information Technology)* (27%), *Education & Research* (22%) and *EPES (Electrical Power & Energy Systems)* (16%). Figure 3 presents in detail the general demographic information of our study.

Fig. 3 Survey general demographic information: **a** age, **b** education, **c** work field, **d** business domain

Considerations and limitations

Surveys in general meet with people reluctance and disinclination especially when there is no apparent gain for them. Taking into consideration the special living and working circumstances under which underlying survey was conducted, justifies attitude and misbelief encountered. Participation rate was far less than the anticipated one based on the dispatched invitation emails. Yet, when time

becomes more precious than usually and pressure more apparent in all aspects of daily life, expectations need to be adjusted accordingly. A greater sample would enhance the severity of our findings as well as their reliability. However, this was not made feasible without violating the life-cycle condition set as one of the core criteria when designing our survey.

The aforementioned conditions raise some considerations regarding the emotional state of the participants directly affecting their security attitude and noted behavior. Answers related to employee emotions, thoughts and beliefs were affected by the COVID-19 lockdown situations. Moreover, the cyber incidents were very much likely related to the current cyber security reality created due to COVID-19 crisis.

Respect toward both anonymity and privacy of the participating individuals and the collaborating organizations, forbid a number of questions that could promote rather interesting results related to nationality, gender, etc. and their relation to cyber security. Additionally, in an effort to keep the questionnaire short and to the point, free text answers were avoided, while the few ones used presented rather revealing results.

A number of admissions were also made aiming to maintain a short completion time duration and, at the same time, simplify our approach toward the rather complex technological solutions and corresponding terminology used by information security. For instance, in the question related to remote access to corporate networks, we asked participants to select one of the provided choices and not a combination of them. In some cases, different access options are provided by the same organizations to their employees. The same applies also for hardware assets used for remote working.

Detailed survey results

Remote working possibility

Based on the responses provided to our survey, *1 out of 4 participants was unable to work from home prior to COVID-19 crisis*. This proportion persisted for managers, whereas for researchers and IT professionals was limited down to 1 out of 7. Almost half (47.06%) of the employees of the banking & financial sector reported they had no teleworking possibility prior to the pandemic. Around the same percentage (45.24%) was noticed to the EPES sector, whereas the IT and telecommunications sectors proved to be better established regarding remote working, as exhibited in Fig. 4a.

These percentages, examined in combination with the job nature and digitalization level of the participating enterprises (as mentioned before, mostly European innovators and research founders), were not the anticipated ones. Moreover, they underline a number of additional difficulties specific business sectors had to deal with during the pandemic since they lacked the means and possibly the mentality of remote working (Fig. 5).

Fig. 4 **a** Remote working possibility per business domain. **b** Remote working possibility per working position

Fig. 5 Security awareness and readiness **a** overall and **b** per business domain

Security awareness and readiness

During a period when cyber-crime spikes, security threats, frauds and breaches have been brought to light and recommendations have been given by cyber security organizations and experts around the globe (COVID-19, Info Stealer & the Map of

Threats – Threat Analysis Report 2020, Home working: preparing your organization and staff 2020, Working From Home—COVID-19—ENISA n.d.), it comes as a surprise that 53% of the participants report not to have received any security guidelines from their employers regarding working from home. Even more troubling is the fact that 44.44% of the employees that had no remote working possibility and, possibly experience, up until the crisis, state they had no security advice on their new working reality.

Failing to advice, enforce and train your workforce, especially during demanding periods and under stressful circumstances, is a worrisome indication about both the organizational change management procedures and the security awareness and training program. It consequently promotes doubts of whether the corporate security officers were aware of the noticeable cyber-crime increase and realized the risks at hand in combination with the new employment status. No matter what the case is, they underperformed in keeping everyone informed and supported making a key blow to the overall cyber security organizational culture.

On the other hand, enterprises which exhibited a better organizational culture level and top management support by providing a number of cyber security guidelines during the coronavirus period, *focused mainly on the corporate network access management* (Virtual Private Network, VPN, usage and avoidance of wireless connections) and *less on the assets safety* (password protection, locking, software updating, phishing emails) as depicted in Table 1.

This organizational trend is also verified by the network access management policies applied this period. Figure 6 presents gathered responses based on which *direct access to corporate network and assets was limited down to 11%*, whereas in the rest of the cases participants report other more robust and secure access solutions.

Hardware assets management and security

Only to enhance the severity of the previous survey finding, around 36% of the assets used for teleworking were personal ones and 16% were corporate ones under no MDM (Mobile Device Management) system for security policies enforcement. Therefore, summing up to a percentage of 52% of *hardware assets with no strict security rules and apparent surveillance used for remote working* gaining access to

Table 1 Top security guidelines provided to the participants during COVID-19 working from home experience

Top security guidelines	%
Use VPN (virtual private network) to access corporate network	32.52
Ensure password security and usage	12.19
Be careful of phishing emails	10.56
Avoid usage of unsecure wireless connections	10.56
Lock working station (PC, laptop, etc.) when unattended	10.56
Ensure daily software updates	7.31

Fig. 6 Network access management and security

corporate networks. To make numbers look worse, a 23% of the corporate assets were partly managed giving some space to security violations and bridges.

As presented in Fig. 7b, these percentages significantly vary for different business domains underlining their differentiation both in cyber security mentality and resilience. Focusing on the three dominating sectors of our survey (the ones presented an adequate answer sample), *IT, Education & Research and EPES*, the

Fig. 7 a Hardware assets used for remote working. b Hardware assets used for remote working per business domain

corresponding percentage (personal assets and corporate assets under no management system) equals to 36.62%, 73.68% and 52.38% respectively.

Security features of the hardware assets used by the participants for their teleworking experience are being presented in Fig. 8. The first revealing observation is that a short, but nonetheless present, percentage of 3.41% *lacked the basic security rules*. Around 1.89% of the assets presented no access or authentication mechanism (password protection or two-factor authentication). Although, it appears to be an encouraging statistical result, security experts would argue that the effect of those security measures is almost diminished when *no automatic locking mechanism is enabled*, as appears to be the case for 1 out of 2 assets used, or their *usage is allowed to other individuals* apart from the authorized ones, approximately 15% of our sample.

Fig. 8 **a** Hardware assets security features. **b** Hardware assets security features per business domain

Another noticeable observation is that *more advanced security techniques*, such as two-factor authentication (27.65%) and hard disk encryption (30.68%), *are yet to be adopted by most corporations*, whereas established software solutions, such as antiviruses (66.29%), are more widespread. Figure 8b comes to shed some light on the three dominating business sectors of our survey regarding security innovation and adaptability where IT appears to be dominating while leaving EPES significantly behind (Fig. 9).

Regarding the antispam software solutions, it would not be safe to reach to conclusions based on our survey responses since many organizations use a centralized approach, usually bound with the emailing solution at hand, which is totally transparent to the end-user.

Change management

Most organizations, in their effort to adapt to special circumstances of this unprecedented for our century health crisis, had to obtain new technological solutions to facilitate their operations and the new employment reality. Consequently, some *employees were requested to use applications or services that they were unfamiliar with while remote working*. Based on our survey results, this was the case for 1 out of 6 of the participants.

Although, this is certainly a good flexibility indicator for the enterprises, their way of communicating these changes and facilitating their workforce in adapting to them strongly affects the effectiveness of their change management strategies. In almost half of the cases, instructions were provided via email. Second in the communication list was the usage of corporate portals and websites (34.78%), whereas the more interactive and usually fruitful, *training method was only used with a percentage of 8.70%*.

Remote working collaboration

Working from home should by no means be translated to working alone. Collaboration and teamwork need to be facilitated and promoted, especially during this time period when general isolation is mandated as the only defense against the virus spread. Companies are expected to provide all means necessary to assist their

Fig. 9 **a** Participants requested to use new applications or services due to remote working overall and **b** the way they were informed

employees in being productive, effective and cooperative. Current collaboration solutions offer numerous possibilities from teleconferencing and real-time chatting to document management and real-time co-authoring, project management and task scheduling. Based on our survey, *2 out of 3 participants report that the organization they work for has adopted a corporate collaboration tool*. This proportion, more or less, is verified for most of the examined business domains, as exhibited in Fig. 10c, proving a trend favoring such edge-technological solutions toward the virtual office envision.

Security incidents management

Participants were asked to report if they have encountered any cyber security threats during the COVID-19 crisis without revealing any sensitive information related to those incidents. Around *1 out of 5 reported to have come up against some kind of security threat with number one being the phishing attacks (15.15%)*.

Fig. 10 **a** Participants using a collaboration solution provided by the employer, **b** collaboration possibilities offered, **c** Adoption of collaboration solutions per business domain

Looking closer into these results and focusing on the three business domains with a better participation rate (Fig. 11b), we notice that *security threat percentages drastically increase moving from the IT to Education & Research and finally to the EPES sector*. It is noticeable that variations in this case are significant. For example, spyware/virus infection cases appear six times more often in the EPES sector compared to the IT, whereas phishing attempts three times more often. Another yet interesting observation is that *data loss and hacking is mainly reported by IT employees* raising

Fig. 11 **a** Cyber security threats encountered by the participants. **b** Cyber security threats encountered by the participants per business domain. **c** Cyber security threats encountered by the participants per age group

considerations if that is really the case. Were they the only ones to experience such kind of cyber-crime attempts or were they the only experienced ones to notice, defend themselves and report such incidents? These observations examined along with the hardware assets management and security results presented in the previous paragraphs prove the effectiveness of the security policies and measures of certain IT corporations against the rest of the participating domains.

Another data analysis approach, depicted in Fig. 11c, reveals *a cyber-threat report increase when moving from younger to older participants*. Reported ransomware and spyware/virus infections reach up to 6.25% and 8.33% for respondents aged 45–54 years old, while the corresponding rates for 25–34 years old are limited down to 1.25% and 2.50%. Does this imply that younger technology users are more familiar with cyber-dangers and, therefore, exhibit a deeper security resilience and consciousness or does it signify the exact opposite? Does youth naivety and ignorance reflect on their security behavior and affect their ability to notice and react against cyber-crime? Are older employees, due to their longer cyber-existence and internet exposure, more targeted and victimized in the digital world? Is it more demanding for them to catch up with technological evolution and maintain their resistance against cyber-perils?

Employee climate

The satisfaction each employee has toward his/her employer, other colleagues, information security itself directly affects his/her security behavior. A number of agreement Likert questions were contained within our survey in an attempt to poll the thoughts, emotions and feelings of the participants since these parameters are key factors in the overall security behavior and attitude of individuals. Based on collected responses, *employees present no clear preference between working from home and going to the office*. They appear to have no definite fondness over these distinct working circumstances and notice no radical differences to their productivity and collaboration.

On the other hand, there is *a clear positive notion towards their employer and its reaction and support during this rather peculiar time period*. Most of the respondents expressed their satisfaction regarding their working experience during this pandemic verifying the technological and security readiness and flexibility of most corporations as noted in previous sections of present study (Fig. 12).

Key findings

Each question of underlying survey was targeting specific security culture factors in an attempt to evaluate their readiness level and bring to light dark points or even failures of the existing security infrastructure and principles. Summarizing and comparatively analyzing the results presented in detail in previous paragraphs, we conclude in the following key findings:

Fig. 12 Employee climate results

- Remote working, whenever feasible due to the job nature, is not always offered as a possibility to the employees. Specific business domains appear more reluctant in embracing this new working reality, whereas others are pioneers in this field trying to enforce its establishment by adopting technological solutions facilitating remote collaboration and cooperation.
- Information security is an integral part of synchronous organizations exhibited mainly via cyber security technological solutions, such as firewalls, antivirus software, intrusion detection systems, security operation centers and so on. Yet, human factor is still not recognized as a core element of the cyber security chain as indicated both by the cyber-threat incident reports and the lack of guidelines and continuous information regarding security dangers.
- Individuals are more aware of security issues and countermeasures than in the past proving a profound security culture and information technology familiarity. As a result, personal assets are better equipped and safeguarded but some basic security principles are still violated indicating that training and support are always needed to enforce current security status and awareness level.
- As a remainder of the previous business reality, greater emphasis is being given to corporate network perimeter enforcement while neglecting assets management and security, especially of the remote ones. Aforementioned security approach is a result of the monolithic past, were a corporate network could be fortified to simulate a “close” system, the safest of all. However, it contradicts with the well-known security truth that “a chain is only as strong as its weakest link” and, nowadays, with teleworking used widely, this danger becomes more apparent. Each asset gaining access to a corporate network constitutes an unbreakable part of it able to give access to intruders and become a means of penetration and violation of its security fortification (Fig. 13).
- Corporations are much more flexible nowadays thanks to the technological solutions at hand adapting to demanding and, in some cases, violent changes of the business environment. This innovative behavior needs to be expanded also to

Fig. 13 Some of the remarkable comments provided by the participants

information security, where radical deviations occur almost daily, to keep pace with development and remain safe at all times.

Conclusion and future work

Security culture is cultivated via a long and time-consuming procedure affected by various factors with different weights. Its foundations lie on the security awareness and readiness exhibited under all circumstances transforming and adapting over time and changes. This survey aimed to evaluate cyber security culture exhibited by organizations from different countries and business domains when teleworking became a necessity due to the COVID-19 crisis. One of the biggest emergencies of our century. Results demonstrate significant variations among participating individuals and corporations proving that information security, although gradually evolving, has a long and fastidious path until becoming an unbreakable part of business operations and workforce reality.

Organizations demonstrate a decentralization notion over the last decades, moving from one building to compounds, from one city to multiple complexes in the suburbs and to the province. The same approach is also depicted in the business digital world where corporate networks are broadened and employees with remote working stations of all kinds become core elements of a wireless net. Information security and corresponding culture need to evolve and adjust offering policies, procedures, measures and solutions applicable to the new reality. Employees awareness, familiarity and expertise on security issues needs to be encouraged and cultivated via continuous training programs and active participation on modern security bridge simulations and exercises. Cyber-crime evolves exploiting each opportunity arisen throughout time and space and so should our cyber security culture.

While in the twenty-first century, it comes as a surprise that: 1 out of 4 employees was unable to work remotely; 1 out of 3 participants has no collaboration mechanism when teleworking; almost half of the hardware assets used for working from home bear no strict security rules or comply with minimal security policies; one can encounter still unprotected hardware assets; 1 out of 2 individuals report no automatic locking mechanism for business working stations; highly educated and experienced technology users report phishing, ransomware and spyware violations. And what probably was the most striking of all: 53% of the participants report not to have received any security guidelines from their employers regarding working from home during this crisis.

Scientific research should emphasize on security adjustments required by different business domains and corporations toward the virtual office envision which tends to become a necessity nowadays. Greater focus is requested on individual security characteristics such as behavior, attitude, awareness and compliance, and research is mandated on quantifying these mainly quality indicators for having a reliable cultural approach toward cyber security. Human factor is the key to information security progress and remains yet uncharted.

Supplementary Information The online version contains supplementary material available at <https://doi.org/10.1057/s41284-021-00286-2>.

Acknowledgement This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832907.

Funding This work has been co-funded from the European Union's Horizon 2020 research and innovation program under the EnergyShield project "Integrated Cyber security Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures", Grant Agreement No 832907.

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

- ActionFraud—National Fraud and Cyber Crime Reporting Center. 2020. *Coronavirus scam costs victims over £800k in one month*. ActionFraud—National Fraud and Cyber Crime Reporting Center. 06 03. Accessed 04 16, 2020. <https://www.actionfraud.police.uk/alert/coronavirus-scam-costs-victims-over-800k-in-one-month>.
- ActionFraud—National Fraud and Cyber Crime Reporting Center. 2020. *Coronavirus-related fraud reports increase by 400% in March*. ActionFraud—National Fraud and Cyber Crime Reporting Center. 03 20. Accessed 04 16, 2020. <https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march>.
- Draugalis, JoLaine Reiersen., Stephen Joel Coons, and Cecilia M. Plaza. 2008. Best practices for survey research reports: A synopsis for authors and reviewers. *American Journal of Pharmaceutical Education*. <https://doi.org/10.5688/aj720111>.
- ENISA. 2020. *ENISA Threat Landscape 2020—Phishing*. Technical, ENISA. <https://www.enisa.europa.eu/publications/phishing>.
- Europol. 2020. *COVID-19: FRAUD*. 04 02. <https://www.europol.europa.eu/covid-19/covid-19-fraud>
- Europol. 2020. *Pandemic profiteering: how criminals exploit the COVID-19 crisis*. Europol. <https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis>.

- Fowler Jr, Floyd , and Floyd J. Fowler. 1995. *Improving survey questions: Design and evaluation*. Thousand Oaks, CA: Sage.
- Georgiadou, Anna, and Spiros Mouzakitis. 2020. Working from home during COVID-19 crisis. Athens, 06 02. https://forms.office.com/Pages/AnalysisPage.aspx?id=-_YTkoGZDU-4MPRIqwUcDASY11B1exdAudIH6_4tf5UQIRLU5ORFZIUdRPMEICRFBDMkE2N0QxVC4u&AnalyzerToken=5RKuzWbBIeHwFFNt24m4FKPAU9OBqy0H.
- Georgiadou, Anna, Spiros Mouzakitis, and Dimitrios Askounis. 2020a. Working from home during COVID-19 crisis – A Cyber-Security Culture Assessment Survey. Athens: Mendeley Data, 06 02. <https://doi.org/10.17632/59tp8sdgr8.2>.
- Georgiadou, Anna, Spiros Mouzakitis, and Dimitris Askounis. 2020b. Designing a cyber-security culture assessment survey targeting critical infrastructures during covid-19 crisis. *International Journal of Network Security & Its Applications (IJNSA)* 13 (1): 33–50. <https://doi.org/10.5121/ijnsa.2021.13103>.
- Georgiadou, Anna, Spiros Mouzakitis, Kanaris Bounas, and Dimitrios Askounis. 2020c. A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*. <https://doi.org/10.1080/08874417.2020.1845583>.
- Hui, David S., Esam I. Azhar, Tariq A. Madani, Francine Ntoumi, Richard Kock, Osman Dar, Giuseppe Ippolito, et al. 2020. The continuing 2019-nCoV epidemic threat of novel coronaviruses to global health—the latest 2019 novel coronavirus outbreak in Wuhan, China. *International Journal of Infectious Diseases* 91: 264–266. <https://doi.org/10.1016/j.ijid.2020.01.009>.
- International Labour Organization (ILO). 2020. *ILO Monitor: COVID-19 and the world of work. Second edition*. International Labour Organization (ILO). https://www.ilo.org/wcmsp5/groups/public/dgreports/dcomm/documents/briefingnote/wcms_740877.pdf_36
- Interpol. 2020. *INTERPOL warns of financial fraud linked to COVID-19*. Lyon, 03 13. <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19>.
- National Cyber Security Centre. 2020. *Home working: preparing your organisation and staff*. National Cyber Security Centre. 03 17. Accessed 04 17, 2020. <https://www.ncsc.gov.uk/guidance/home-working>.
- Reason Labs. 2020. *COVID-19, Info Stealer & the Map of Threats—Threat Analysis Report*. Reason Labs. 03 09. Accessed 04 16, 2020. <https://blog.reasonsecurity.com/2020/03/09/covid-19-info-steal-the-map-of-threats-threat-analysis-report/>.
- Velavan, Thirumalaisamy P., and Christian G. Meyer. 2020. The COVID-19 epidemic. *Tropical Medicine and International Health* 25 (3): 278–280. <https://doi.org/10.1111/tmi.13383>.
- World Health Organization (WHO). 2020. *WHO Director-General's opening remarks at the media briefing on COVID-19*. Geneva: World Health Organization (WHO).
- Willis, Gordon B. 2004. *Cognitive interviewing: A tool for improving questionnaire design*. Thousand Oaks, CA: Sage.
- n.d. *Working From Home—COVID19—ENISA*. ENISA—European Union Agency for Cybersecurity. Accessed 04 17, 2020. <https://www.enisa.europa.eu/topics/WFH-COVID19?tab=details>.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.