Viewpoint

COVID-19 and Cybersecurity: Finally, an Opportunity to Disrupt?

Ana Ferreira[1,2*], PhD; Ricardo Cruz-Correia[1,2*], PhD

[1]CINTESIS, Faculty of Medicine, University of Porto, Porto, Portugal
[2]MEDCIDS, Faculty of Medicine, University of Porto, Porto, Portugal
[*]all authors contributed equally

Corresponding Author:
Ana Ferreira, PhD
CINTESIS
Faculty of Medicine
University of Porto
Rua Plácido Costa, s/n
Porto, 4200-450
Portugal
Phone: 351 220426964
Email: amlaf@med.up.pt

Related Articles:
Preprint: https://preprints.jmir.org/preprint/21069
Peer-Review Report by David W Chadwick (Reviewer B): https://med.jmirx.org/2021/2/e29417/
Peer-Review Report by Anonymous: https://med.jmirx.org/2021/2/e29068/
Peer-Review Report by Anonymous: https://med.jmirx.org/2021/2/e29414/
Peer-Review Report by Anonymous: https://med.jmirx.org/2021/2/e29096/
Peer-Review Report by Anonymous: https://med.jmirx.org/2021/2/e29070/
Authors' Response to Peer-Review Reports: https://med.jmirx.org/2021/2/e29517/

Abstract

COVID-19 has challenged cybersecurity to meet the ultimate need of guaranteeing the privacy and security of human beings. Although personal and sensitive health data are needed to better understand, detect, and control the disease, many related cybersecurity challenges and vulnerabilities require further analysis and proper discussion. The aims of this viewpoint are to explore the consequences of COVID-19 on cybersecurity and health care as well as to foster awareness regarding the need for a change in paradigm on how cybersecurity is approached. Education and information technology literacy are important when they are suitably provided; however, they are certainly not a complete solution. Disruption needs to occur at the core of human-device interactions. Building trust, providing novel means to interact with technology (eg, digital humans), and supporting people—the most important cybersecurity asset—are only some of the recommendations for a more human and resilient approach to cybersecurity, during or after the pandemic.

(JMIRx Med 2021;2(2):e21069) doi: 10.2196/21069

KEYWORDS

COVID-19; cybersecurity; challenges and disruption; data protection; privacy; health data

Introduction

The COVID-19 pandemic has created many difficult challenges and required many decisions to be made to quickly adapt to the situation on a daily basis. However, COVID-19 has serious consequences related to cybersecurity and the human right to privacy, security, and even physical integrity. Many of these consequences are directly related to the treatment of the disease, such as sharing of personal and sensitive data for research and treatment or contact tracing of patients; meanwhile, other consequences can be indirectly linked with the pandemic but are equally dangerous. These consequences include the continued treatment of other diseases while patients are confined to their homes and the increased vulnerabilities and risks of physical and web-based security when people rely on the internet for most of their daily activities (eg, working from home, homeschooling, shopping on the web, home banking, contact with friends and family, exercising, and entertaining).

Within the literature, it is recommended that data analyses should be performed in accordance with the law and with respect for privacy, which can increase public trust and adherence [1,2]. The need for transparency is even greater when personal and sensitive data are used for contact tracing using smartphone technology. Contact tracing apps are powerful tools that can help limit disease transmission during a pandemic, enforce quarantine rules, notify users of risk zones, or warn infected people [3]. However, contact tracing apps present significant privacy concerns because they collect personal data, such as location, which can also be used to perform a high degree of surveillance and harm individuals' privacy [4]. An adequate balance between anonymity and data quality and integrity, with adequate transparency by certified authorities, is required.

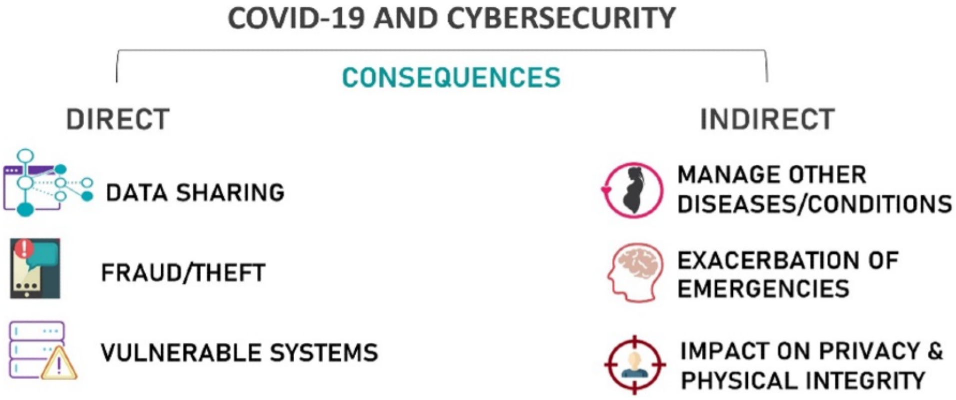
Although many other diseases or conditions may require constant support and treatment, the COVID-19 pandemic has also exacerbated emergencies that may not be promptly addressed, such as chronic, oncological, or mental health conditions [1,5]. Health care professionals must opt for alternative (possibly less secure) means to support their patients, such as teleconsultation, email, and social networks [6].

These cybersecurity issues are just the beginning. In the first part of this viewpoint (COVID-19, Cybersecurity, Privacy, Security, and Safety), the authors identify and discuss cybersecurity challenges and consequences that COVID-19 has brought to the surface that need urgent attention. This part is based on our published work [7]. In the second part (Required Changes in Cybersecurity), recommendations for novel approaches to address the identified issues are advanced to foster a change in the current cybersecurity paradigm. This section comprises the authors' original recommendations and are specific to this viewpoint.

COVID-19, Cybersecurity, Privacy, Security, and Safety

The authors have categorized the identified cybersecurity issues as direct and indirect consequences of COVID-19, as presented in Figure 1.

Figure 1. Direct and indirect consequences of COVID-19 for cybersecurity as identified by the authors.


COVID-19 AND CYBERSECURITY
CONSEQUENCES
DIRECT
INDIRECT
DATA SHARING
FRAUD/THEFT
VULNERABLE SYSTEMS
MANAGE OTHER DISEASES/CONDITIONS
EXACERBATION OF EMERGENCIES
IMPACT ON PRIVACY & PHYSICAL INTEGRITY

Direct Consequences of COVID-19

Data Sharing

The most pressing challenges related to contact tracing focus on the balance between sharing and maintaining the privacy of personal data, which is crucial but difficult to achieve [3,4]. Contact tracing apps should not be made available without proper risk assessment and data integrity verification [8]. If data are anonymized, integrity is more difficult to guarantee because anonymized data are more susceptible to undetected interference; thus, these data are not useful and trustable for the proposed health care goal. Data integrity can only be achieved by forfeiting some degree of privacy, ideally to a trusted entity.

The lack of information technology and cybersecurity literacy can also make it more difficult for most individuals to adequately install and use contract tracing apps, while the apps themselves may integrate technical security vulnerabilities and risks [9]. For instance, the most commonly used protocol in tracing apps is Bluetooth, which has known and intrinsic vulnerabilities, such as a lack of boundary control. Bluetooth signals can traverse walls and cars, and individuals who receive the signals may not be actually in contact with an infected person. The balance between frequent false positive or negative results may need adjustment according to the evolution of the pandemic, as it may be safer to obtain more false positives than false negatives, especially if the virus is very contagious [10].

Finally, even if these contact tracing apps gain wide adherence and use, questions arise. What is the effective return or benefit for individual or public health? How can this return or benefit be measured in relation to the loss of privacy? Now is the right time to answer these questions.

Fraud and Theft

There has been a great increase in false messages associated with the COVID-19 pandemic [11]. These messages feed on the spread of misinformation, "fake news," fear, isolation, and lack of awareness to turn the confined population into a vulnerable target for those types of attacks [12] and persuade victims to give away money, personal data, and credentials (eg, phishing, ransomware, false fundraising campaigns) [13]. Further, when people are isolated, they tend to buy more products on the web; therefore, attackers can take advantage of fraudulent product delivery messages. It should be noted that security data breaches performed during this time will not only be exploited now but will have an extremely wide impact in the future, as this exploitation will continue for a long time after the pandemic has subsided.

In drastic times such as the COVID-19 pandemic, other serious issues may arise. International espionage and sabotage can become more common. Recent examples are the lack of proper management of vaccination procedures as well as the reliance on large multinational companies to fairly distribute and sell the vaccines [14,15]. The provision of preventive means and appropriate public policies to detect and avoid these issues is essential to protect people's lives.

Vulnerable Systems

Most health care systems are underbudgeted, use obsolete technology, and are noninteroperable, and they often lack the latest patches and adequate configurations [16,17]. The COVID-19 pandemic has cleared the way for attackers to better exploit these vulnerabilities. The stress placed on these systems is very high; additionally, there is a risk of shortage of equipment due to the high number of hospitalized patients at one time. European Union countries are required to comply with the General Data Protection Regulation (GDPR) to protect personal data. Unfortunately, this is still not common practice, and organizations attempt to address the situation with few or no resources and, most importantly, with no expert knowledge [18].

Indirect Consequences of COVID-19

Managing Other Non–COVID-19–Related Diseases and Emergencies

Although the COVID-19 pandemic is a serious situation worldwide, with the looming threat of collapse of health care systems, it is not possible to put the treatment of other diseases on hold. Patients with chronic, oncological, mental health, obstetrical, and other health care conditions must be treated. Teleconsultation and web-based medical advice are available [19,20], but at what price for patients' privacy? The security systems in most home infrastructures are not prepared to adequately control and protect personal and sensitive data.

Increased Risks to Physical Security and Integrity

One serious consequence of the COVID-19 pandemic is the isolation of a large part of the world's population. Fifty years ago, when information was only communicated through the mail and landline telephone companies, cybersecurity was not an issue. Currently, however, almost all daily activities have become virtual. Still, in an ideal world where all home infrastructures are secured and people take the necessary precautions to protect their data and physical integrity, cybersecurity will still be an issue. This is due to the complex relationships between humans and technology. Some common examples are listed below:

- Risky behaviors may arise, as simultaneously assessing every interaction and message from different contexts, 24 hours per day 7 days per week, can create stress and lead people to make poor and unsafe decisions.
- Different contexts (eg, personal, professional, familiar, educational) can easily lead to confusion and mistakes.
- Different populations are affected differently (eg, older people, minority groups, children, and adolescents). Words such as cyberbullying, fake profiles, impersonation, trolling and *Zoombombing* (disrupting Zoom conferences) may come to mind [21]. Home infrastructures are not prepared from a security standpoint, and adults working from home are burdened and distracted, leaving younger people more vulnerable.
- People are engaging in frequent telephone or video calls, and they may often forget to consider the environment they are in and who may be listening. From balconies and gardens, or even through doors or walls, information can slip out more frequently than we may think. Espionage and theft can and often do occur undetected [22].
- Unlocked sessions or devices and microphones or cameras connected at unwanted times can share more personal information than they should.

Required Changes in Cybersecurity

During the pandemic, the world has been experiencing one wave of COVID-19 after another; still, governments, companies, and the public are all focused on returning to their "normal" prepandemic routines. However, in cybersecurity (as in other areas), "normal" involves low budgets, lack of awareness and education, lack of proper infrastructures, and inability to adapt to different uses by various people and in various contexts. "Normal" also means that privacy and security are still among the greatest challenges in human-computer interactions [23].

Change is crucial, and the COVID-19 pandemic has stressed this even more; however, this change is difficult to achieve. Hence, like a small pebble in a large pond, the authors wish to use this viewpoint to disrupt existing ideas and paradigms and promote other perspectives for discussion in cybersecurity as well as its associated technologies and procedures.

Cybersecurity literacy and education are essential, even more so during pandemic times. One way to achieve these goals is generating scientific research, such as this viewpoint, to raise awareness, provide recommendations, and try new or improved solutions. However, the current times demand web-based, easy, fast, accurate, and objective but personalized and meaningful information and education that is adapted to the situation and context and to the target population [24]. Due to the unpredictable nature of human behavior and actions, humans are an important element and the main enablers of the level of cybersecurity that each system can and will have [24].

However, education is not sufficient. People have thrived for thousands of years by successfully using tools, and not because they are experts or have complete knowledge about every tool or activity [25]. Why should their relations with technology be much different? Several factors may come into play in human-device relations (eg, security, usability, design, efficiency, demographics, previous interactions); however, even when these factors are addressed, adequate and secure use of technology may still not be possible. There is a pervasive line that permeates all these relations and factors that is known as *trust*. Although this can be a *feared* (subjective) subject in computer science, trust can be established on the web because technology has a social presence to which people respond [26]. However, research fails to capture the reasons why end users choose to trust or distrust systems [27] and what factors contribute to trust [28]. A solid formalization of computational trust, to explain how relationships develop through interactions across a range of web-based contexts, would provide enhanced web-based security [29]. Researchers and developers should be brave enough to consider trust development within technology design by providing features that support end users in evaluating the trustworthiness of the technology, helping to promote proper use of technology, and minimizing the frequency of security incidents [30].

By addressing the previous issue, much more can be understood in terms of personality traits, tendency to trust, and propensity toward manipulation and victimization in human-device relations. This will certainly enable the implementation of more adequate strategies to address one of the most critical unsolved problems in cybersecurity—social engineering.

Further, advancements in trust in human-device relations can open the way to more confident use of innovative solutions such as high-fidelity digital humans [31]. These advancements can work to promote *second life* or augmented reality contexts and to improve privacy, for instance, of children and adolescents, with their many interactions using videoconferencing tools (eg, homeschooling, exercise, music lessons).

Some of the discussed ideas can take longer to study and implement; however, while this is being done, the authors suggest the use of anonymous "digital twins" to easily and quickly test interactions between users and technology. Mockup interfaces complemented with anonymous surveys available on the web can be quickly developed to test the security, privacy, and usability of a technology by a large sample of people with a wide range of experiences, characteristics, and behaviors.

Limitations of this viewpoint are its space constraints and the fact that it is based on an original paper published in conference proceedings. Because of this, a more technical and detailed discussion about the introduced subjects is not possible.

Conclusion

This viewpoint has highlighted the many cybersecurity challenges associated with COVID-19; however, none of the identified challenges are new but have clearly been exacerbated by the pandemic. Therefore, the problems existed before the pandemic, and still no adequate solutions are available. Change and disruption needs to occur at the core of human-device interactions and relations, with a focus on trust and on how humans have thrived with each other over thousands of years, even in threatening situations.

We should take this opportunity to face those challenges before they pile on top of the pandemic toll. In extreme situations, it is normal that exceptions need to be made to prioritize specific parts of society or infrastructures. However, this needs to be accomplished in a transparent and controlled way so that after the exceptional situation subsides, people can easily take back their fundamental right to privacy [32], the loss of which has affected so many lives in the past. We must also claim the right of trust in technology, with more appropriate and improved cybersecurity, for a safer and healthier human population.

Conflicts of Interest

None declared.

References

1. Jawaid A. Protecting older adults during social distancing. Science 2020 Apr 10;368(6487):145-145. [doi: 10.1126/science.abb7885] [Medline: 32273460]
2. Ienca M, Vayena E. On the responsible use of digital data to tackle the COVID-19 pandemic. Nat Med 2020 Apr 27;26(4):463-464 [FREE Full text] [doi: 10.1038/s41591-020-0832-5] [Medline: 32284619]
3. Abeler J, Bäcker M, Buermeyer U, Zillessen H. COVID-19 contact tracing and data protection can go together. JMIR mHealth uHealth 2020 Apr 20;8(4):e19359 [FREE Full text] [doi: 10.2196/19359] [Medline: 32294052]
4. Li J, Guo X. Global deployment mappings and challenges of contact-tracing apps for COVID-19. SSRN Journal. Preprint posted online on May 26, 2020. [doi: 10.2139/ssrn.3609516]
5. Yao H, Chen J, Xu Y. Patients with mental health disorders in the COVID-19 epidemic. Lancet Psychiatry 2020 Apr;7(4):e21 [FREE Full text] [doi: 10.1016/S2215-0366(20)30090-0] [Medline: 32199510]
6. Now, You Can Consult a Doctor on WhatsApp: Govt Issues Telemedicine Guidelines. India.com. 2020 Mar 26. URL: https://www.india.com/news/india/now-you-can-consult-a-doctor-on-whatsapp-govt-issues-telemedicine-guidelines-3981377/ [accessed 2021-03-26]
7. Ferreira A, Cruz-Correia R. Cybersecurity in pandemic times: challenges and opportunities. 2020 Jul 21 Presented at: 12th International Conference on e-Health; July 21-23, 2020; Croatia p. 135-142.
8. Nature. COVID-19 digital apps need due diligence. Nature 2020 Apr 30;580:563 [FREE Full text]
9. Larson RS. A path to better-quality mHealth apps. JMIR mHealth uHealth 2018 Jul 30;6(7):e10414 [FREE Full text] [doi: 10.2196/10414] [Medline: 30061091]
10. Ng PC, Spachos P, Plataniotis K. COVID-19 and your smartphone: BLE-based smart contact tracing. ArXiv. Preprint posted online on May 28, 2020.
11. WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. 2020 Apr 23. URL: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance [accessed 2021-03-26]

12. Khan NA, Brohi SN, Zaman N. Ten deadly cyber security threats amid COVID-19 pandemic. TechRxiv. Preprint posted online on May 11, 2020. [doi: https://doi.org/10.36227/techrxiv.12278792.v1]
13. Ahmad T. Corona virus (COVID-19) pandemic and work from home: challenges of cybercrimes and cybersecurity. SSRN Journal. Preprint posted online on April 5, 2020. [FREE Full text] [doi: 10.2139/ssrn.3568830]
14. COVID-19 vaccines and corruption risks: preventing corruption in the manufacture, allocation and distribution of vaccines. United Nations Office on Drugs and Crime. URL: https://www.unodc.org/documents/corruption/COVID-19/Policy_paper_on_COVID-19_vaccines_and_corruption_risks.pdf [accessed 2021-02-15]
15. INTERPOL warns of organized crime threat to COVID-19 vaccines. INTERPOL. 2020 Feb 12. URL: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines [accessed 2021-02-15]
16. Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 2018 Jul;113:48-52. [doi: 10.1016/j.maturitas.2018.04.008] [Medline: 29903648]
17. Goniewicz K, Khorram-Manesh A, Hertelendy AJ, Goniewicz M, Naylor K, Burkle FM. Current response and management decisions of the European Union to the COVID-19 outbreak: a review. Sustainability 2020 May 08;12(9):3838. [doi: 10.3390/su12093838]
18. Ferreira A. GDPR: what's in a year (and a half)? In: Proceedings of the 22nd International Conference on Enterprise Information Systems - Volume 2: ICEIS. 2020 Presented at: 22nd International Conference on Enterprise Information Systems; May 5-7, 2020; Online p. 209-216.
19. Kavoor AR, Chakravarthy K, John T. Remote consultations in the era of COVID-19 pandemic: preliminary experience in a regional Australian public acute mental health care setting. Asian J Psychiatr 2020 Jun;51:102074 [FREE Full text] [doi: 10.1016/j.ajp.2020.102074] [Medline: 32294583]
20. Gerke S, Shachar C, Chai PR, Cohen IG. Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. Nat Med 2020 Aug;26(8):1176-1182 [FREE Full text] [doi: 10.1038/s41591-020-0994-1] [Medline: 32770164]
21. Chen L, Utkucan B, Jeremy B, Gianluca S. A first look at Zoombombing. ArXiv. Preprint posted online on September 8, 2020. [FREE Full text]
22. The scale and impact of industrial espionage and theft of trade secrets through cyber. Publications Office of the European Union. 2018. URL: https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en [accessed 2021-03-25]
23. Stephanidis C, Salvendy G, Antona M, Chen JYC, Dong J, Duffy VG, et al. Seven HCI grand challenges. Int J Hum Comput Interact 2019 Jul 01;35(14):1229-1269. [doi: 10.1080/10447318.2019.1619259]
24. Maalem Lahcen R, Caulkins B, Mohapatra R, Kumar M. Review and insight on the behavioral aspects of cybersecurity. Cybersecur 2020 Apr 21;3(1) [FREE Full text] [doi: 10.1186/s42400-020-00050-w]
25. Siegrist M, Gutscher H, Earle T. Perception of risk: the influence of general trust, and general confidence. J Risk Res 2006 Aug 15;8(2):145-156. [doi: 10.1080/1366987032000105315]
26. Hoff, Bashir M. Trust in automation: integrating empirical evidence on factors that influence trust. Hum Factors 2015 May;57(3):407-434. [doi: 10.1177/0018720814547570] [Medline: 25875432]
27. Kulyk O, Milanovic K, Pitt J. Does my smart device provider care about my privacy? Investigating trust factors and user attitudes in IoT systems. In: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. 2020 Oct Presented at: 11th Nordic Conference on Human-Computer Interaction; October 25-29, 2020; Tallinn, Estonia p. 1-12. [doi: 10.1145/3419249.3420108]
28. Kelton K, Fleischmann KR, Wallace WA. Trust in digital information. J Am Soc Inf Sci 2008 Feb 01;59(3):363-374. [doi: 10.1002/asi.20722]
29. Jones HS, Moncur W. The role of psychology in understanding online trust. In: Psychological and Behavioral Examinations in Cyber Security. Hershey, PA: IGI Global; 2018:109-132.
30. Borchert A, Ferreyra NED, Heisel M. Building Trustworthiness in Computer-Mediated Introduction: A Facet-Oriented Framework. New York, NY, USA: Association for Computing Machinery; 2020 Presented at: International Conference on Social Media and Society (SMSociety'20); July 2020; Toronto, ON p. 39-46. [doi: https://doi.org/10.1145/3400806.3400812]
31. High fidelity digital humans. Didimo. URL: https://mydidimo.com/ [accessed 2021-02-15]
32. Pesce M. Privacy in the time of Covid-19. IEEE Spectr 2020 May;57(5):23-23. [doi: 10.1109/mspec.2020.9078452]

Abbreviations

GDPR: General Data Protection Regulation

Edited by E Meinert; submitted 04.06.20; peer-reviewed by D Ferreira, Anonymous, Anonymous, Anonymous, Anonymous; comments to author 11.09.20; revised version received 02.10.20; accepted 08.03.21; published 06.05.21

Please cite as:
Ferreira A, Cruz-Correia R
COVID-19 and Cybersecurity: Finally, an Opportunity to Disrupt?
JMIRx Med 2021;2(2):e21069
URL: https://xmed.jmir.org/2021/2/e21069
doi: 10.2196/21069
PMID: