Int. Cybersecur. Law Rev. (2020) 1:51–61
https://doi.org/10.1365/s43439-020-00014-3

Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats

Alina Škiljić

Received: 1 September 2020 / Accepted: 21 September 2020 / Published online: 12 October 2020

Abstract Coronavirus disease 19 (COVID-19) has influenced all aspects of life, and cybersecurity becomes more relevant than ever. The transition to remote information technology (IT) solutions has opened a plethora of possibilities for cyber incidents and attacks, with the most "popular" now apparently being phishing schemes and ransomware attacks. Remote working applications, such as file-sharing and collaboration tools, numerous personal devices accessing the network, higher email traffic, cloud solutions and similar COVID-19-influenced shifts in work organization might all lead to data breaches, as well as loss and theft of data, resulting in huge financial and reputational losses. In addition to losing valuable business information, money, and consumer confidence if cyber-attacked, companies are also under threat of General Data Protection Regulation (GDPR) fines if the cyber attack results in a personal data breach. It seems that many European countries have recognized cybersecurity as being crucial during the COVID-19 pandemic, while, unfortunately, Croatia has stayed completely silent on the pandemic-related cybersecurity hazards; it has simply left companies to figure out their own ways of reacting to the increased cyber threats, without even warning individuals.

Keywords COVID-19 · Cyber attacks · Data breaches · Data protection · Croatia

1 Introduction

Who would have predicted a global pandemic in 2020? And yet, here we are—Coronavirus disease 19 (COVID-19) has influenced all aspects of life, in-

A. Škiljić (✉)
Faculty of Law (LLM), Associate in Zagreb office of the international law firm CMS, CIPP/E, University of Zagreb, Zagreb, Croatia
E-Mail: alina.skiljic@gmail.com

cluding healthcare, work and education, as well as law. Always relevant, but now more so than ever, is the discussion on cybersecurity. The pandemic has created an unforeseen demand for the workforce to move out of corporate premises and students out of their schools into virtual environments, making people less careful and systems more vulnerable. Transitioning to remote information technology (IT) solutions has opened up a plethora of possibilities for cyber incidents and attacks, which have already shown an increase.[1] In addition to the existing risks of infection or theft of valuable information and the cybersecurity implications linked to remote working and education, the high volume of health data being processed during the pandemic, supported by COVID-19-related technology tools (such as contact tracing apps[2]), open up heretofore less explored opportunities, which seem to be particularly attractive to cyber criminals.

This was recognized by many governments, and cybersecurity regulators promptly followed with warnings and recommendations addressed to the public and private sector and individuals. However, it seems that Croatia has not (yet) recognized cybersecurity as being threatened. In a nutshell, cybersecurity is not a highly discussed topic in Croatia, not even after a high-profile cyber attack earlier this year on INA, a European oil company with a leading role in the Croatian oil business, which suffered a ransomware attack infecting and encrypting some of the company's backend servers [19]. It has been continuously emphasized that Croatia lacks enough experts in the cybersecurity field [18], which is why it is not surprising that the Croatian authorities have been completely silent on the pandemic-related cybersecurity hazards. This article also refers to the cyber implications of remote working and their increase during the pandemic, as well as the liability of companies under the General Data Protection Regulation (GDPR)[3] for personal data breaches that might occur following cyber attacks, while emphasizing the lack of the appropriate response in Croatia.

2 Remote working-related cyber threats

Remote access to companies' systems and data is crucial for remote working to function. While, fortunately, today's technology facilitates the adaptability of the work situation to extraordinary circumstances such as ones caused by the pandemic, they also increase the vulnerability of IT system infrastructures. The remote work environment creates quite compelling opportunities for cyber criminals.[4] Firstly, it is highly unlikely that all companies can provide their employees with a work computer (i.e. a portable device owned by the company with direct access to the server and a degree of cyber protection equal to company-owned computers used at the work-

[1] See, e.g. [16]; see also [17].

[2] Croatia released its contact tracing app called "Stop COVID-19" in July 2020.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1.

[4] See, e.g. [3].

place) to use in their homes. Thus, some employees use their personal devices for remote access to the server, as well as their private Wi-Fi networks. These personal endpoints (laptops, tablets, computers) and home wireless connections are potential entry points for cyber criminals, if insufficiently secure [20]. Using personal devices for work—also known as bring your own device (BYOD)—whereby employers as data controllers stay liable for any personal data processed on the BYOD for work-related purposes poses certain data protection compliance issues [1], and this "system" is now being increasingly used in remote work environments. Also, generally, personal devices have a lower degree of cybersecurity protection; employees outside the data security system are rarely entirely aware of the cyber threats they may face. It is questionable whether employees know what security protocols are in place on their devices or how efficient their Wi-Fi limiting antivirus supports are, etc. [2, 23].

Likewise, interruptions in remote access are not rare, irrespective of the quality of the remote systems today: in such cases, employees under pressure of work assignments might start downloading company files on their personal computers instead of in the company's cloud, to be able to continue to work if remote access is interrupted or decelerated. Moreover, with the increased "home-distractions" (e.g. children, pets) and COVID-19-related concerns (e.g. health, finances, etc.), data security is not the focus of employees' attention, and quite reasonably so. In such surroundings, employees might become negligent and lose sight of safeguards against cyber attacks, especially if they are not properly trained in cybersecurity. It is thus unsurprising that phishing attacks—which simply use email or text messages to trick people into giving them personal information (e.g. log-in credentials)—are on the rise, as cyber criminals are exploiting individuals' fears and need for information [24]. If an employee is a phishing victim, the company's control over its data can be disrupted—and the company can consequently be legally liable for data breaches, as will be further explained. To put it simply: what started with a simple email click by an employee or a transmission over an unsecured network might result in losing valuable information and money. In addition, the foreseen and installed computational capacities may not sufficiently support the entire workforce simultaneously, which is why companies started upgrading their capacities by recklessly implementing cloud technologies, which increases potential security risks; this is especially relevant in the case of infrastructure-as-a-service (IaaS)[5] cloud solutions, whereby security control is divided between cloud service providers and companies.

To summarize, remote working applications, such as file-sharing and collaboration tools (e.g. Zoom), numerous personal devices accessing the network, higher email traffic, cloud solutions and similar COVID-19-related shifts in work organization might all lead to data breaches, as well as loss and theft of data, resulting in huge financial and reputational losses.

[5] See, e.g. [5].

3 Croatian cybersecurity legal regime

Croatia's cybersecurity regulation revolves around the European Union (EU) Network and Information Security Directive[6] implemented by the national Act on Cybersecurity of Operators of Essential Services and Digital Services Providers (NIS Act)[7]. Essential services comprise services of social and economic importance and functioning of the digital market, e.g. finance[8], energy[9] and healthcare. The NIS Act applies to providers of these essential services, regardless of whether they are public or private entities, the country of their registered seat, size, organization and ownership (OES), as well as to digital service providers (DSP), but only if they have a registered seat in Croatia or a representative and if they are not a micro- or small-sized enterprise[10]. OESs and DSPs are obliged to implement appropriate, state-of-the-art organizational and technical measures to avoid security incidents in the network and information systems, and must notify the competent authority in the event of major cybersecurity incidents.[11] Regarding DSPs, these security measures must be implemented by the providers of the online marketplace, internet search engines and cloud computing services. The prevention and response to cybersecurity threats is in the authority of the Information Systems Security Bureau, the Office of the National Security Council and the National CERT[12], the latter being in charge of the protection of the public information systems' security.

Further, the Information Security Act (ISA) envisages measures and standards of information security, areas of information security and supervisory activities and applies to state authorities, local and regional authorities, legal entities with public authorities that use classified and unclassified data and to natural and legal persons that obtain access to or handle classified and unclassified data.[13] The conduct of the electronic communications market participants is further regulated by the Electronic Communications Act (ECA), which provides rules on the establishment, mainte-

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194.

[7] Act on cybersecurity of operators of essential services and digital service providers, Official Gazette 64/18; Regulation on cyber security of operators of essential services and digital service providers, Official Gazette No. 68/18 see also [14].

[8] The security obligations of the providers in the financial services market are regulated by the Credit Institutions Act, Official Gazette 159/13, 19/15, 102/15, 15/18, 70/19, 47/20 and the Payment System Act, Official Gazette 66/18.

[9] Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency (Text with EEA relevance) OJ L 326 also imposes certain security obligations on the participants of the electricity and gas market.

[10] NIS Act, Article 3. Measures for DSPs are defined by the European Commission Implementing Regulation pursuant to Art 16(8) of the NIS Directive.

[11] The OESs are, depending on the sector, supervised by the competent authorities (e.g. the Ministry of Environment and Energy, the Croatian National Bank, Croatian Financial Services Supervisory Agency, Central Office for the Development of the Digital Society etc.).

[12] National CERT deals with the incident if one party to the incident is in a .hr Internet domain or is a Croatian citizen using "hosting" services of a foreign service provider.

[13] Information Security Act, Official Gazette 79/07.

nance, use of the electronic communications infrastructure, continuity of provision of services and the protection of the users' rights.[14] According to the ECA, the Public Electronic Communication Service Providers are obliged to protect the security of their services, while the Public Electronic Communication Network Providers are in charge of undertaking network integrity measures to ensure uninterrupted provision of services. The implemented measures have to ensure that personal data may be accessed only by authorised persons for lawful purposes, protect the transferred or stored personal data from accidental or unlawful destruction, accidental loss or change, and unauthorised or unlawful storage, processing, access or disclosure and ensure that security policies are applied in relation to the processing of personal data.[15] The authority supervising the behaviour in the electronic communications market is the Croatian Regulatory Authority for Network Industries (HAKOM). A separate legal regime also exists for the electronic identification and trust service providers.[16]

Outside the cybersecurity-specific regulations, and applicable irrespective of the industry, all companies are subject to the GDPR's rules and principles on ensuring data security and, as such, must implement technical and organizational measures to ensure confidentiality and integrity of personal data. These measures are analyzed further below under paragraph V. and the violations thereof must be reported to the Croatian Personal Data Protection Agency (AZOP) if they resulted in a data breach.[17] Criminal liability for cyber attacks is envisaged under the Criminal Act.[18]

4 Croatia's (non-)response to increased cybersecurity threats

As the title of this article suggests, Croatia has not reacted properly (or at all) to the increased cyber threats resulting from shifting to remote working. Although Croatia does have the cybersecurity regulation in place, which is primarily the consequence of joining the EU, it seems that cybersecurity is still not of an imperative nature in Croatia, or at least is not recognized as being at risk during COVID-19. What is especially odd is that, of the many recommendations and guidelines issued for combating the health-related and other implications of COVID-19, cyber threats have not been addressed. Public authorities and the cybersecurity entities have been silent on this topic, even though the Minister of Interior argued back in 2019 that

[14] Electronic Communications Act, Official Gazette 73/08, 90/11, 133/12, 80/13, 71/14, 72/17.

[15] Electronic Communications Act, Official Gazette 73/08, 90/11, 133/12, 80/13, 71/14, 72/17.

[16] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC OJ L 257 and the Act on the Implementation of the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Gazette 62/17.

[17] GDPR, Article 33; [15].

[18] Criminal Act, Official Gazette 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, Section XXV, see also [10].

cybersecurity is "a security priority and a crucial factor in the development of society and the state" [25].

For comparison, several EU jurisdictions issued warnings and recommendations for cybersecurity during COVID-19. Hungarian authorities and cyber bodies warned about spam emails and false information, and issued recommendations for a secure home office, including, e.g. disallowing the use of Zoom by lawyers [29]. Poland issued general guidance on security regarding the use of devices, email, networks and the cloud in the context of remote working [27]. Romania has issued a number of rules to be considered during the COVID-19 pandemic, such as using only encrypted communication channels (SSL VPN – a type of virtual private network (VPN) that uses the Secure Sockets Layer protocol which enables devices with an internet connection to establish a secure remote-access, IPsec VPN – a type of VPN relying on a group of protocols that are used together to set up encrypted connections between devices), assessing possible security risks and informing the employees thereof, appointing a person who provides remote support to employees in the event of technical or security errors, etc. [32]. Slovakia suggested using only platforms with a good reputation for videoconference calls (e.g. no Zoom) and instructed employees to regularly communicate with their employers and with the colleague(s) responsible for IT and cybersecurity, as well as to notify all suspicious events and circumstances (phishing emails, suspicious calls and SMSs, non-standard computer functioning, etc.) [28]. Slovakia also suggested that infrastructure security must be a priority for employers, and they should provide employees with guidelines about working from home safely. Slovenia's guidelines for employers on secure remote work indicate the need to make employees aware of the cyber threats by implementing secure access to the organization's network, updating exposed systems, creating or adapting an incident response plan and setting up tools for teamwork, while the Slovenian Data Protection Agency published guidelines on the protection of data while working from home [30, 31].

It seems that many European countries have recognized cybersecurity as being crucial during COVID-19 while, unfortunately, Croatia has not; it has simply left companies to figure out their own ways of reacting to the increased cyber threats, without even warning individuals. It is thus left to each employer to decide and implement its own cybersecurity measures and to determine the terms and conditions of assignments as well as the fulfilment and control of remote work. In this escalated technology environment, companies must be even more diligent when ensuring that appropriate security measures are in place for remote working, all in alignment with the requirements for security in processing personal data envisaged by Article 32 of the GDPR and under risk of huge monetary fines for data breaches, as exemplified below.

5 Liability for personal data breaches arising from cybersecurity attacks

GDPR, amongst others, imposes obligations on data controllers and data processors to keep personal data secure and private. Integrity and confidentiality of data

is a fundamental principle, or, better said, an imperative for data processing.[19] The main purpose of the requirement to ensure data security is to avoid any personal data breaches. Under GDPR, personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed".[20] As can be seen from this definition, a security breach precedes the personal data breach, which must lead to one of the above-mentioned negative events. Thus, depending on the assessment of the cyber risks, appropriate security measures, such as the pseudonymisation and encryption of personal data, measures to ensure confidentiality, integrity, availability and resilience of processing systems and services, as well as measures to restore availability in a timely manner where a physical or technical incident occurs, must be put in the place.[21]

The two most notable recent cases involving a personal data breach occurring as a result of cyber attacks due to insufficient technical and organizational measures to ensure information security are ones led by the United Kingdom's (UK) Information Commissioner Office (ICO) against Marriott International Inc (Marriot) and British Airways. The Marriot cyber attack resulted in various personal data contained in approximately 339 million guest records being globally exposed [21]. British Airways suffered an incident involving user traffic to the British Airways website being diverted to a fraudulent site through which customer details of approximately 500,000 customers were harvested by the attackers [22]. Although fines imposed by the ICO on the Marriot (EUR 110,390,200) and British Airways (EUR 204,600,000) are not final and are still to be decided on, they illustrate quite well how serious data breaches are considered and how cybersecurity should be considered a top priority. In addition to the presented examples, there have been at least 87 fines issued by the EU's data protection authorities with respect to the security of data, and they all resulted from insufficient technical and organizational measures to preserve data security [26].

Not all cyber attacks will result in GDPR liability: to explain, companies can suffer a security breach without being in violation of the law—namely Article 32 GDPR. To avoid liability, data controllers, in line with the accountability principle[22], must prove that security measures were appropriate to the risk, in such way that the cyber attack or other security breach occurred even with adequate security measures having been put in place. This is triggered by the personal data breach notification to the competent data protection authority, which is the obligation of data controllers unless it is unlikely that a personal data breach will result in a risk to the rights and freedoms of natural persons.[23] Under certain conditions, data subjects must also be notified of a breach.[24] What is notably "tricky" is that a data controller might be liable for personal data breaches that occurred within the processing performed by another

[19] Article 5 (1) (f) GDPR.

[20] Article 4 (1) (12) GDPR.

[21] Article 32 GDPR, see [7].

[22] Article 5 (2) GDPR.

[23] Article 33 GDPR; see also [11].

[24] Article 34 GDPR.

subject under its instructions—data processor—when such processing involves the data controller's personal data.[25] To illustrate: if an employer outsources the payroll services, and if the service provider suffers a cyber attack resulting in a personal data breach of a controller's employees, the data controller might also be liable for this breach in accordance with their obligation to contract only reliable data processors that are likewise under obligation to implement appropriate technical and organizational security measures.[26]

Thus, in addition to losing valuable business information, money (e.g. due to ransomware attacks, companies might be forced to pay a certain amount of money to hackers to retrieve their data in unencrypted forms and, at the same time, they might lose money due to the impossibility of performing business without the access to data) and consumer confidence if cyber-attacked, companies are also under threat of huge GDPR fines[27] if the cyber attack results in a personal data breach. In line with the broad liability of companies acting as data controllers, they should therefore be extremely diligent not only with respect to their own cybersecurity systems, but also with those implemented and maintained by service providers whose services they use.

6 Final remarks

It is evident that efforts to combat COVID-19 should also be combined with efforts to combat the increased cyber threats arising. Although COVID-19 opens space for various kinds of cyber attacks, the most "popular" now seeming to be phishing schemes and ransomware attacks, the latter being especially intrusive in many respects—just recently, a woman in Germany died during a ransomware attack on the Duesseldorf University Hospital [4, 8, 33]. Companies should audit their cybersecurity systems, strengthen their cybersecurity policies to tackle these issues and, perhaps most importantly, educate their employees accordingly. Remote work and the limited possibilities to control the workplace, combined with curtailed diligence of individuals arising from their fears and almost desperate need for information due to the pandemic, force companies to envisage and implement long-term IT solutions.

In line with the risk-based approach required by both the NIS Act and the GDPR[28], companies should consider cyber risks during remote work more intensively than under usual circumstances, and adapt their cybersecurity policy to this new environment—where the risk is higher, the cybersecurity measures must be stronger. The technology stack with special appreciation of the increased "people risk" in a home-environment must be duly taken into consideration when implementing cybersecurity measures. Multi-factor authentication should be used wherever possible,

[25] Article 28 GDPR, see also [12], see also [1].

[26] Article 28 GDPR.

[27] Fines of up to EUR 10,000,000 or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, can be imposed on data controllers and data processors for not complying with data security obligations, Article 83 (4) GDPR.

[28] See, e.g. [6].

avoiding the simple and weak password-based authentication.[29] Additional security layers should be implemented in all apps used by a company, and collaboration apps deemed insecure should be avoided (such as Zoom). Companies should implement VPN solutions with encrypted network connection, while well-established communication channels between employees and IT staff could facilitate a prompt response in the case of a cyber incident. Nevertheless, companies should audit the security measures implemented by their service providers and due care should be taken with regard to privacy and data protection, implementing solutions such as privacy by design and default.[30] Data controllers should remember the burden of proof that adequate measures were in place in the event that a personal data breach lies on them.

Indubitably, each company is responsible for the implementation of strong remote access security controls. However, the Croatian Government and cybersecurity regulators should issue additional guidance and recommendations for companies and individuals. Cybersecurity awareness should grow in proportion to the cybersecurity issues, and Croatia should put more effort into raising this awareness—although there are many ways in which companies can strengthen their cybersecurity framework, employees' negligence is often beyond their reach—and public alertness could contribute to a more diligent attitude among individuals towards cybersecurity issues, thus elevating the Croatian cybersecurity scheme to a greater level.

References

1. Ustaran E (ed) (2018) European data protection: law and practice, 2nd edn. International Association of Privacy Professionals, Portsmouth
2. Adelmann F, Gaidosch T (2020) Cybersecurity of remote work during the pandemic. https://www.imf.org/~/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.ashx. Accessed 1 Sept 2020
3. Ahmad T (2020) Corona virus (COVID-19) pandemic and work from home: challenges of cybercrimes and cybersecurity. In: SSRN electronic journal. https://ssrn.com/abstract=3568830. Accessed 13 Sept 2020
4. Green A (2018) Ransomware and the GDPR. Netw Secur 3:18–19. https://doi.org/10.1016/S1353-4858(17)30030-2
5. Bhardwaj S, Jain L, Jain S (2010) Cloud computing: A study of infrastructure as a service (IAAS). In: IJEIT 2(1):60–63. https://www.academia.edu/1181740/Cloud_computing_A_study_of_infrastructure_as_a_service_IAAS_.Accessed. Accessed 9 Sept 2020
6. Cole MD, Schmitz S (2019) The interplay between the NIS directive and the GDPR in a cybersecurity threat landscape. In: University of Luxembourg law working paper no. 2019-017. https://ssrn.com/abstract=3512093. Accessed 12 Sept 2020
7. Huth D, Matthes F (2019) Appropriate technical and organizational measures: identifying privacy engineering approaches to meet GDPR requirements. In: information security and privacy (SIGSEC). https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/5/. Accessed 8 Sept 2020
8. Richardson R, North MM (2017) Ransomware evolution, mitigation and prevention. In: international management review, faculty publications 4276. https://digitalcommons.kennesaw.edu/facpubs/4276. Accessed 10 Sept 2020

[29] See, e.g. [3]; See also [9].

[30] Article 25 GDPR; see also [13].

9. Weil T, Murugesan S (2020) IT risk and resilience—cybersecurity response to COVID-19. In: IT professional 22: 4–10. https://www.researchgate.net/publication/341583723_IT_Risk_and_Resilience-Cybersecurity_Response_to_COVID-19. Accessed 10 Sept 2020
10. Zlatović D (2016) Kaznenopravna zaštita u području prava intelektualnog vlasništva i kompjutorskog prava u Republici Hrvatskoj (Criminal legal protection in the field of intellectual property and computer related rights in the Republic of Croatia). Pravni Zapisi Pravnog Fak Univ Union Beograd 6(2):394–427
11. European Data Protection Board (2018) Guidelines on personal data breach notification under regulation 2016/679, 18/EN. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Accessed 8 Sept 2020
12. European Data Protection Board (2020on) Guidelines 07/2020 on the concepts of controller and processor in the GDPR. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. Accessed 8 Sept 2020
13. European Data Protection Board (2019on) Guidelines 4/2019 on article 25 data protection by design and by default. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en. Accessed 8 Sept 2020
14. (2015) The national cyber security strategy of the republic of Croatia. https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Croatian%20National%20Cyber%20Security%20Strategy%20. Accessed 1 Sept 2020
15. Croatian Data Protection Agency (AZOP). Personal data breach notification form. https://azop.hr/zbirke-osobnih-podataka/detaljnije/izvjesca-o-povredi-osobnih-podataka. Accessed 10 Sept 2020
16. Truta F (2020) Cybersecurity incidents up 23 % after COVID-19 forced businesses to switch to remote work, in: business insights blog. https://businessinsights.bitdefender.com/cybersecurity-incidents-up-23-after-covid-19-forced-businesses-to-transition-to-remote-work. Accessed 1 Sept 2020
17. WHO WHO report on fivefold increase in cyber-attacks and urging vigilance. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance. Accessed 1 Sept 2020
18. Sprečić E (2019) Nemamo dovoljno stručnjaka za kibernetičku sigurnost (We do not have enough cybersecurity experts). In: Večernji list. https://www.vecernji.hr/premium/nemamo-dovoljno-strucnjaka-za-kiberneticku-sigurnost-1311620. Accessed 10 Sept 2020
19. (2020) The announcement of the INA group on ransomware attack. https://www.ina.hr/en/announcement-cyber-attack/. Accessed 17 Sept 2020
20. Seymour H (2020) A pandemic and remote working: cyber security under the microscope. In: IFSEC GLOBAL. https://www.ifsecglobal.com/cyber-security/a-pandemic-and-remote-working-cyber-security-under-the-microscope/. Accessed 6 Sept 2020
21. ICO (2019) Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach (9 July 2019). https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/. Accessed 7 Sept 2020
22. ICO (2019) Statement: Intention to fine British Airways £183.39m under GDPR for data breach (8 July 2019). https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/. Accessed 8 Sept 2020
23. Security Magazine (ed) (2020) Increasing cybersecurity gaps and vulnerabilities due to remote work during COVID-19 (2020). https://www.securitymagazine.com/articles/92571-increasing-cybersecurity-gaps-and-vulnerabilities-due-to-remote-work-during-covid-19. Accessed 13 Sept 2020
24. Panda Media Center (2020) 43 COVID-19 cybersecurity statistics, panda media center. https://www.pandasecurity.com/mediacenter/news/covid-cybersecurity-statistics/. Accessed 1 Sept 2020
25. (2019) Announcement of the Croatian Minister of Interior. https://vlada.gov.hr/vijesti/bozinovic-kiberneticka-sigurnost-je-sigurnosni-prioritet-i-presudan-faktor-razvoja-drustva-i-drzave/25955. Accessed 13 Sept 2020
26. The list and summary of the imposed GDPR fines. https://www.enforcementtracker.com/. Accessed 10 Sept 2020
27. UODO (ed) Guidelines of the Polish Data Protection Authority (UODO) on cybersecurity and remote work. https://uodo.gov.pl/pl/138/1459. Accessed 10 Sept 2020 (https://uodo.gov.pl/pl/138/1513)
28. Guidelines of the Slovakian National Security Authority on cybersecurity and remote work. https://korona.gov.sk/varovania-narodneho-centra-kybernetickej-bezpecnosti-sk-cert/. Accessed 10 Sept 2020
29. Guidelines of the Hungarian Cybersecurity Institute (Nemzeti Kibervédelmi Intézet) on remote work. https://nki.gov.hu/en/. Accessed 10 Sept 2020

30. Guidelines of the Slovenian National Cyber Security Incident Response Centre (SI-CERT—nacionalni odzivni center za kibernetsko varnost) on secure remote work. https://www.cert.si/en/. Accessed 10 Sept 2020
31. Guidelines of the Slovenian Data Protection Authority (Informacijski pooblaščenec) on the protection of data while working from home. https://www.ip-rs.si/novice/kako-zascititi-osebne-podatke-ko-delamo-od-doma-1180/. Accessed 10 Sept 2020
32. Guidelines of the Romanian Cybersecurity Authority (Serviciul Tehnologia Informației și Securitate Cibernetică) on secure remote working. https://stisc.gov.md/ro. Accessed 10 Sept 2020
33. Wetsman N (2020) Woman dies during a ransomware attack on a German hospital. In: The Verge. https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity. Accessed 19 Sept 2020