The Challenges to Information Security in Croatian Chamber of Economy during COVID-19 Pandemic

Dražen Lučić
Croatian Chamber of Economy, Zagreb, Croatia
dlucic@hgk.hr

***Abstract* - The paper deals with analysis of both challenges to information security Croatian Chamber of Economy prior and after COVID-19 pandemic and the results of the measures that were taken in order to counter fought with those challenges by means of state-of-the-art Information and Communication Technology solutions. COVID-19 pandemic has rapidly and significantly changed ecosystem for social and business activities. Croatian Chamber of Economy, as legal entity with public authorities, has been affected by numerous limitation which have directly impacted effectiveness of the business processes. The analysis of the measures and activities undertaken by Croatian Chamber of Economy in order to keep a high level of information security during COVID-19 pandemic and experience from that time period is described in the paper. Pre-emption of possible events with negative influence on business activities, as well as risk management and crisis management plan, are some of the most important prerequisites for a successful continuation of business activities during a crisis such COVID-19 pandemic has been. Beside the solutions based on ICT technology, permanent education of the employees is the activity that must not be omitted.**

Keywords – Information Security, Cyber Security, COVID-19 pandemic, legal entity with public autorities, Croatian Chamber of Economy

I. INTRODUCTION

As information and communication technology (ICT) have advanced in their capabilities, and especially with the greater availability of high-speed internet, remote working has grown in its use as a new mode of work in the past several decades [1]. However, prior to the COVID-19 pandemic, remote working was not a widely used practice [2]. Although the number of employees who worked from home at least half of their working time grew in last ten years, remote working at that time was below five percent of the total workforce in both US and Europe [3]. Remote working has, in fact, been a "luxury for the relatively affluent" [4], such as higher-income earners and "white-collar workers" e.g. executives, managers, or professionals.

Because of this situation, prior to COVID-19, most workers had little remote working experience; nor were they or their organizations prepared for supporting this practice. Now, the unprecedented outbreak of the COVID-19 pandemic in 2020 has required people across the world into being remote workers, inadvertently leading to a de facto global experiment of remote working [6]. Remote working has become the "new normal," almost overnight.

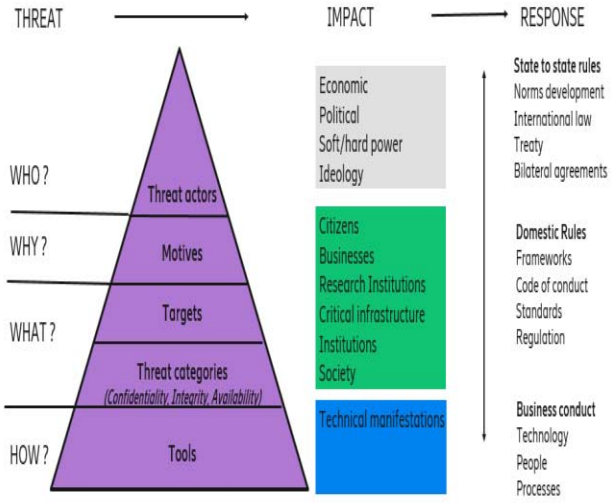

Figure 1. The cyber threats at electronic communications market

In order to cope with the new social and business situation, many companies, state and public institutions, legal entities, etc. have found own solutions for remote working and new business process. These solutions have been mostly based on ICT and electronic communications. Electronic communications, empowered with high speed data connections and high data rates, have shaped society and markets. Today we speak about digital/information society, digital transformation and new industrial revolution. Digitalization in now an intrinsic part of every country's sustainable economic and social development. However, digital transformation and the expansion of the digital ecosystem also comes with increased cybersecurity risks, especially for but not limited to the small and media enterprises and legal entities that may lack adequate cyber resilience against constantly evolving digital cyber threats. While the private sector and policy makers are continuously working to increase the resilience of digital infrastructure, software and devices top make harder for malicious actors to succeed in their objectives, this is not sufficient to break the growing trend and decrease cyberthreats (Figure 1) [6].

In parallel to this significant technology change in electronic communications there is an another interesting process ongoing. European Union (EU) commission published several documents that strongly influences data processing business as well as information security. In 2016 EU Parliament introduced General Data Protection Regulation (GDPR) [7]. GDPR is a data protection law which came in force in 2018 with influence on information security and EU single digital market as well. This has a huge impact not only huge impact on electronic communications market regulation in but also information security in the areas where new technology solutions are applied for business processes.

II. Information Security at Legal Entities with Public Authorities

The transformation to digital society and digital economy is one of the results of ongoing process of digitalisation and globalisation. On one side this process creates enormous opportunities for business but on another side could become obstacle or even a huge hurdle in implementation of new technologies. The process is accompanied by a growing public awareness and concern for the importance of information security that also comprises cyber security [8].

Information security is one of the key issues to be addressed by legal entities It gives the importance of transparency and the risk of personal data breaches. To overcome possible information security problem, legal entities introduce numerous requirements regarding the confidentiality and security of personal data. This process implies also a number of changes that the legal entities need to implement, particularly in terms of security, privacy, personal data processing and protection as well as user services. Another threat is possible vulnerability user services because of their purpose, especially when legal entity has some public authorities. Some of user services are not applicable in existing telecommunications network due to satisfactory quality of service (QoS) and that might cause difficulties in providing such service by means of remote working. Wide use of mobile internet access via 4G and 5G public mobile telecommunications network might overcome the issue with QoS.

Due to the fact that almost nobody has been prepared for such unprecedented events and situation due to COVID-19, strengthened in Croatia by strong earthquakes in 2020, remote working at legal entities in Croatia in common haven't been prepared for neither organisational nor security challenges of remote working. In the same time, the users have expected the same QoS as it was the case prior to COVID-19 [9]. Lack of procedures and experience for such situation at legal entities has caused confusion and stoppage of usual business processes. Those legal entities that have had state-of-the-art ICT infrastructure and skilled employees at both IT and corporate security department, adapted quickly to "new normal" eco-system thus providing services with a good QoS and keeping a high level of information security at the same time. The complete new eco-system has been to cyber threat environment but that has been the challenge that the legal entities had to take on their shoulders (Figure 2).

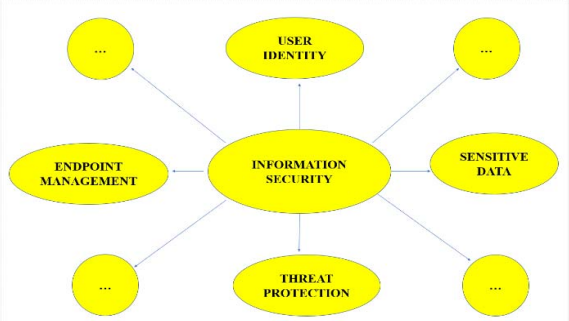

Figure 2. Information security at legal entities

III. Information Security at Croatian Chamber of Economy during COVID-19 Pandemic

Croatian Chamber of Economy (Hrvatska gospodarska komora – HGK). as legal entity with public authorities [10] with headquarter in Zagreb, has experienced severe challenges in the area of information security during COVID-19 pandemic, emphasized by strong earthquakes in Zagreb and its vicinity in March and December 2020. Given the constant threat and responses to cyber-attacks, it has been essential that HGK was technically prepared and with skilled employees who knew how to conceptualise cybersecurity threats, impacts, and responses [11].

Department for information security (OIS) at HGK already beginning of the year 2020 prepared enough lap-top computers, mobile phones, wi-fi routers and applications for a successful and efficient remote working. Applications have been mostly based on an industrial standard solution, Microsoft Office 365 with enterprise licence that includes, among others, MS Teams for video conference and collaboration as well as the tools like "SharePoint" and "OneDrive" for easy collaboration of remote workers. Accidentally just few months before COVID-19 pandemic officially was declared in Croatia, OIS conducted at HGK a survey in order to find out how employees, infrastructure, organisation and prepared are prepared for the challenges in the areas of both information and cybersecurity. The activity was a part of regular annual review of the Information Security Management System at HGK and the first step in preparation process for ISO 27001 certification.

Out of the results of that survey is shown in the figures 3 and 4, where 413 employees at HGK, who are working on 21 locations throughout Croatia and on 7 locations in Europe and China, answered to the question about the cyber threat(s) that they were exposed to. The result confirms general picture about the cyber threats in both business and private eco-system. The same survey, conducted in February 2023, shown that Spam and Phishing remain to be the most frequent cyber threats at HGK but without any negative impact on business due to educated employees. Meanwhile, the percentage of threats in internet shopping and investment fraud during COVID -19 pandemic decreased by roughly ten percent. "Courier fraud" increased during COVID-19 pandemic. It is interesting that "Romance fraud" has become a growing

problem, exacerbated by the COVID-19 pandemic, but hasn't been reported by any of the employees in the survey neither in 2019 nor in 2023.

Figure 3. Explanation for cyber threats

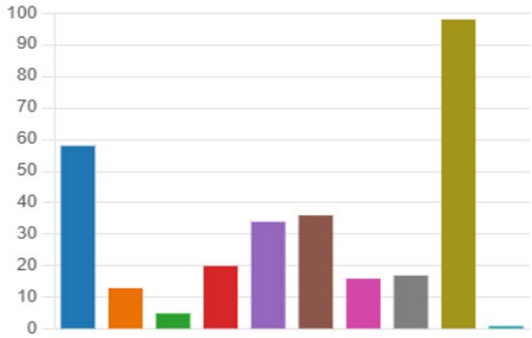

Figure 4. Cyber threats at HGK during COVID-19

IV. The Measures Taken in Order to Increase Level of Information Security at Croatian Chamber of Economy

Mitigating and preventing cyber-attacks are not a trivial task. There are practical approaches that can reduce the risk of cyber-attacks while working remotely. Security is an essential element of trust in new and emerging technologies and a factor that can impact any organization connected to the Internet, but it is not a one-size-fits-all solution and thus not suited to narrow top down prescription. As technologies continue to develop and new technologies continue to emerge, cybersecurity implications need to be considered on a case by case basis. EU has also recognized the importance of information and cyber security. They issued "Cybersecurity Act" in 2019. in order to counter fight with continuously increasing risk on both information security and cybersecurity [12]. The act is the base for many documents and guidelines prepared by EU agency for cybersecurity (ENISA), which include description of the threats to information and cybersecurity and measures how to cope with new challenges be means of state-of-the-art ICT solutions. Therefore, OIS at HGK performed many activities and undertook a lot of measures in order to increase level of information security at HGK during COVID-19 pandemic, especially due to many employees at HGK who over the night became remote workers on numerous locations throughout Croatia [13].

People are considered the weakest link in many security systems. Therefore, developing cybersecurity awareness among users by means of constant training is important to reduce the risks of cyber-attacks on an organization. HGK conducted online education in the area of information and cybersecurity for all employees with 20 to 40 terms yearly in the time period from 2020 to 2023. Number of employees in that period declined from around 550 to around 300.

HGK has implemented and provided to all employees as well as to the selected suppliers representatives Virtual Private Network (VPN), an encrypted communication channel between two points on the Internet to protect the data that is sent and received. HGK VPN provides two aspects of security: confidentiality and integrity and allows HGK to extend security policies to remote workers and suppliers. HGK has strengthened security by Enabling two-vector authentication (TVA), requiring a username and password plus a one-time code sent to user's mobile phone via an authentication app. TVA is an important factor to mitigate against password guessing and theft such as brute force cyber-attacks.

It has been ensured that all devices and equipment firmware/OS are up-to-date with the latest security patches implemented to inoculate them against known vulnerabilities. Regular and up-to-date patches may reduce the risk of a zero-day attack. It has been also ensured that up-to-date anti-malware software was activated in all network connected devices. regular and up-to-date anti-malware may reduce the risk of cyber-attacks caused by malware.

OIS has set a strong company online policy through Information Security Management System (ISMS). Organizational units at HGK had little or no time to prepare for remote work. Robust and comprehensive security policy is necessary to protect data and prevent cyber-attacks. Strong ISMS includes avoiding holding sensitive work conversations in public, use only company-approved video and audio conference lines, etc. The policies should also include a robust and proven recovery plan and backup strategy.

Physical security of home office has been emphasized in HGK ISMS as well. It is important to physically protect home office devices. Practical approaches include ensuring that work devices are not left unattended, use a

lock screen or lock the laptop, always log off devices after use, etc.

It is imperative that legal entities with public authorities protect their valuable data and assets from cyber-attacks by improving their defense. Two important components as regards detecting malicious behavior that can compromise the security and trust of a network are intrusion detection system (IDS) and security incident and event management (SIEM). Typically, an IDS employs anomaly detection, stateful protocol analysis (deep packet inspection), signature matching or a combination of all three techniques (hybrid) to analyze incoming cyber-attacks. Furthermore, it is important for legal entities with public authorities to take a comprehensive approach to cybersecurity and not to view security from a technological perspective only, but in the framework of their business processes.

V. Analysis of Information Security at Croatian Chamber of Economy

During COVID-19 pandemic, OIS at HGK performed yearly online education in the area of information and cyber security for all employees at HGK and selected representatives from the suppliers to HGK. In total more than 100 online sessions have been performed with more than 1 000 participants in total. At the end of each education cycles, OIS has conducted a survey in order to gain a better picture about behaviour, knowledge and experience of the employees at HGK in the area of information and cyber security. There were 364 participants of the survey conducted in the year 2019 and 213 participant of the survey from February 2023. Some of the results obtained from both survey and their comparison are presented in the table 1.

OIS also performed a risk assessment that should identify the typical and most significant threats and their relevance for the business process in HGK during COVID-19 pandemic. The assessment has included the risks due to circumstances of the strong earthquakes in the year 2020 when function of both HGK headquarter in Zagreb and regional office in Sisak were severely disrupted. The assessment presented in the Table 2 [14] includes the following high-level categories of information/cyber security threats and threat actors. The main threat actors are:

- Accidental (Acc.) threat actor, e.g. unintended impact or a side effect from an operation not targeting the operation of a mobile telecommunications network;
- An individual "hacker" (Ind.);
- A "hacktivist" group (Hack. group);
- An organized crime group (Crime group);
- An insider within a telecommunication operator or vendor;
- State or state-backed actor.

Table 1. An comparison of the activities and behaving of the employees at HGK prior and after COVID-19 pandemic

ACTIVITY	YES [%] November 2019	YES [%] February 2023
Have you used a remote access for business activities?	8	93
Have you already attended an (online) education in the area of information security?	2	90
Have you encountered with malicious computer network/software activities?	37	74
Do you back up your computer data regularly?	7	91
Do you take regular software update of your computer?	13	91
Do you take regular software update of your "smart phone"?	48	89
Do you use "OneDrive" for your daily work?	6	93
Do you use "SharePoint" or similar tool for document share?	15	69
Do you use "secure print" in your office?	0	27

The main threats are:

- Compromised confidentiality, including espionage;
- Compromised availability
- Compromised integrity of a service.

Relevance rating is from 1 to 5, i.e. very low, low, medium, high and very high respectively.

Table 2. Summary of findings on main threats to information security at Croatian Chamber of Economy (HGK)

Actors / Threats	Acc.	Ind.	Hack. group	Crime group	Insider	State
Confidentiality	2	4	3	3	4	3
Availability	3	3	3	2	4	2
Integrity	3	3	2	2	3	2

The main threats to information security in HGK don't differ significantly from the main threats in majority of legal entity with public authorities in Croatia. The threat of an intentional cyberattack is high or even very high in a case that main actor behind is a state or a state-backed group. In the case of HGK a threat of a cyberattack from individual hacker or a group of hackers is lower than in majority other legal entities in Croatia due to a preety high level of information and cyber syecurity in HGK, back by a strong ISMS. However, the threat from an insider at HGK or their suppliers is still significantly high and on a similar level to the other legal entities in Croatia.

VI. CONCLUSION

Information security, including cyber security, remains a foundational element of all business activities of the legal entities with public authorities as our societies continue on their path for rapid digitalization. The COVID-19 pandemic was a remarkable and unprecedented event which altered the lives of citizens globally as well as the business processes. Aside from the extraordinary impact on society and business as a whole, the pandemic generated a set of unique cyber-crime related circumstances which also affected society and business. In the same time the impact of cyberattacks and other threats to information security grows, especially because the actors increasingly target critical infrastructure and systems in order to disrupt their functions.

During COVID-19 pandemic, cyber criminals and APT groups have taken advantage of targeting vulnerable people and systems. Furthermore, it is a situation that is unlikely to change in the foreseeable future. Legal entities with public authorities are one the victims of cyber-attacks during the pandemic for various reasons. Hence, it is crucial that these organisations improve protection of their important data and assets from cyber-attacks by leveraging their defence by implementation of comprehensive mechanism and state-of-the-art ICT solutions in order to increase level of information security. Certain practical approaches to reduce the risks of cyber-attacks and possible mitigation techniques are presented in this paper with Croatian Chamber of Economy as the study case.

REFERENCES

[1] V. Di Martino, L. Wirth, „Telework: a new way of working and living", "International labour review", Vol. 129 (5), pp. 529-554, 1990

[2] E.E. Kossek, B.A. Lautsch, "Work–life flexibility for whom? Occupational status and work–life inequality in upper, middle, and lower level jobs", "The Academy of Management Annals", Vol. 12*(*1), pp. 5–36, 2018
https://doi.org/10.5465/annals.2016.0059

[3] "Living and working in Europe", Annual report 2017, 2018 https://www.eurofound.europa.eu/publications/annual-report/2018/living-and-working-in-europe-2017

[4] B. Wang, Y. Liu, J. Qian, S.K. Parker, "Achieving Effective Remote Working During the COVID-19 Pandemic: A Work Design Perspective", "Applied Psyhology", Vol. 70 (1), pp. 16–59, 2021

[5] L. Djurkin-Kőnig, A. Ostojić, A. Delić, "Korporativna sigurnost u okruženju pandemije COVID-19", Poslovno učilište integralna sigurnost i razvoj, Zagreb, Croatia, 2020

[6] D. Lucic, P. Misevic, "An Impact of Implementation of 5 G Technology on Information Security", 44th International Convention on Information, Communication and Electronic Technology – MIPRO, CTI, Opatija, Croatia, 2021

[7] „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)", REGULATION (EU) 2016/679, 27 April 2016
https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016R0679

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, "The Covid-19 Threat Landscape", "Computer Fraud & Security", vol. 2021, Issue 9, pp 10 – 15, 2021

[9] B. Pranggono, A. Arabo, "COVID-19 Pandemic Cybersecurity Issues", "Internet Technology Letters", Volume 4, Issue 2, 2021
https://doi.org/10.1002/itl2.247

[10] Hrvatska gospodarska komora (HGK)
https://www.hgk.hr/

[11] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[12] H. S. Lallie, L. Shepherd, J. R. C. Nurse and A. Erola, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-crime and Cyber-attacks during the Pandemic", "Computer & Security", vol. 105, 2021

[13] J. Zhou, Z. Cao, X. Dong, A.V.Vasilakos, "Working from Home: Cybersecurity in the Age of COVID-19", "IEEE Communications Magazine", vol. 55, no. 1, pp. 26 – 33, 2017

[14] https://cdn.netzpolitik.org/wp-upload/2019/08/2019-07-02-FinalRiskassessmentguidelinesandtemplateforreporting.pdf