Editorial

Cybersecurity and Pandemic Crisis

Prof. Ioan C. BACIVAROV, PhD
President - Romanian Association for Information Security Assurance

1. In early 2020, an unprecedented crisis for modern times has hit all of humanity and brought about huge changes - from lifestyle to doing business: it was the pandemic due to Covid-19.

As mentioned a recent UN document [1], we are facing a global health crisis unlike any in the 75-year history of the United Nations - one that is killing people, spreading human suffering, and upending people's lives. But this is much more than a health crisis. It is a human, economic and social crisis. The coronavirus disease (COVID-19), which has been characterized as a pandemic by the World Health Organization (WHO), is attacking societies at their core.

The Covid-19 pandemic generated a social and an economic crisis, as important as the one at the level of health, through its important consequences worldwide.

From school closures to devastated industries and millions of jobs lost – the social and economic costs of the pandemic are many and varied [2].

As mentioned above, the impact of the Covid-19 pandemic has been broad, affecting general society, economy, culture, ecology, politics, and other areas [3].

In this ***Editorial***, some *effects of the pandemic* on *cyber-security* will be analyzed.

2. Of course, the ways in which the coronavirus pandemic crisis has affected the cyber security of companies and their employees are multiple.

These have been the subject of several studies conducted in the last year by companies and experts specializing in cybersecurity, [4]…[7], for example.

This is not the place for a detailed analysis of them. However, we will highlight some aspects that we think are important.

The coronavirus pandemic has created new challenges for businesses as they adapt to an operating model in which working from home has become the "new normal".

Companies were forced to accelerate their digital transformation, and cybersecurity became a major concern. The great majority of companies have realized that the reputational, operational, legal and compliance implications could be considerable if cybersecurity risks are neglected.

The restrictions imposed by governments in response to the coronavirus pandemic have encouraged employees to work from home. Consequently, technology has become even more important in both our working and personal lives. However, it is found that many organizations still do not provide a "cyber-safe" remote-working environment.

3. According to [4], in the last year a diverse cyber threat landscape appeared the eyes of experts, including:

- Malicious employees working from home with less supervision and fewer technical controls: they may be tempted to carry out a fraud or other criminal activity;
- Cybercriminals recognize that the data security measures currently in place are not sufficiently robust to prevent them from making successful cyber-attacks;
- “Junior” hackers -with less technical skills- but who found the opportunity to test cyberattack packages on a variety of organizations in order to improve their skills;
- The activities of hacktivists (hackers fighting for social and political issues) are adding to the above cybersecurity threats.

Statistics prove that most of these threats intensified during the pandemic, firstly because working from home does not guarantee the same level of cybersecurity as an office environment.

It is obvious that a home working environment does not have sophisticated enterprise prevention and detection measures; furthermore, home Wi-Fi networks are much easier to attack.

As I already mentioned in a previous paper [8], it is important to underline that while organizations continue to purchase and deploy technical controls, not much has been done to focus on the *human side of cybersecurity* - so named *layer 8*.

The term layer 8 is often used by the IT professionals to refer to employees’ lack of awareness and a weak overall cybersecurity culture. Today, it is just as important to secure *human assets - layer 8* - as it to secure layers 1 through 7.

Even prior to the pandemic, human error was already a major cause of “cyber insecurity”. With home working, however, the problem became even greater. IT systems need to adapt to these changes in working practices and the increase in human error. This can be accomplished in many ways such as incorporating time-outs in key information systems, enhancing controls to apply the “four-eyes principle”, enforcing segregation of duties (SOD) or automated controls [4].

4. Under the new conditions generated by the pandemic crisis, employees working from home (using their personal or even corporate-owned computers) must implement the essential cyber-security practices, including: antivirus protection; cybersecurity awareness; phishing awareness; home network security; using *Virtual Private Networks* (VPN); frequent reviews, etc.

Additionally, the companies should identify the security weaknesses of its IT systems using appropriate tests (such as penetration tests), vulnerability scanning a.o. Managers need to keep their business continuity and crisis plans updated and consider cyberattack scenarios.

More advanced measures, such as those based on *Intelligence and Risk management* techniques should be considered. IT managers should encourage proactive use of cyber threat intelligence to identify relevant indicators of attacks (IOC) and address known attacks. Businesses can apply governance, risk and compliance (GRC) solutions for improved risk management [4], [8].

5. In the face of rising threats from malware, phishing and high-tech threat actors, a *cyber resilient company* can position itself as a secure model for data protection customers can trust.

Cyber resilience is the measure of an enterprise's ability to continue with working as normal while it attempts to prevent, detect, control and recover from threats against its data and IT infrastructure [6]. The lessons learned during the pandemic crisis demonstrated that without implementing cyber resilience, without a strong cybersecurity framework, companies are vulnerable and open to cyber-attacks.

6. In the special context generated by the current Covid-19 pandemic, when most activities have moved online, is of crucial importance for all the specialists, professional organizations and companies to develop and consolidate a powerful "*cybersecurity culture*", adapted to the new context. That's why, this was also the main objective - in the last period - of the *Romanian Association for Information Security Assurance (RAISA)*, as the main organization meant to spread the cyber-security culture in Romania.

Among the RAISA activities aimed meant to consolidate the culture of cybersecurity in our country, we can mention the following ones:

- Permanent updating of the RAISA web portals specialized in IT security, namely: Information Security (*www.securitatea-informatiilor.ro*), Cybercrime (*www.criminalitatea-informatica.ro*), Cybersecurity (*www.securitatea-cibernetica.ro*), Networks Security (*www.securitatea-retelelor.ro*) to include changes and requirements in the field of cyber-security in the context of the pandemic;
- Development by RAISA of several projects meant to strengthen the cyber capacity in Romania by raising cybersecurity awareness and improve the skills of criminal justice authorities and private sector in fighting cybercrime. The most recent was the successful project "*Enhance cyber capacity building in Romania for preventing and combating the cybercrime phenomenon*" (2020 - 2021), made in the frame of the United States - Romania Strategic Partnership in cybersecurity.
- Elaboration of works meant to consolidate the cybersecurity culture in our country, from the basic ones, intended for the general public, to the academic ones. We mention in this sense "*Cybersecurity guide*"[1] and the volume "*Dependability of information systems*"[2]).
- Elaboration of studies, meant to highlight the need for high level education in the field of cybersecurity, both nationally and internationally. Particularly important and appreciated in this regard was the study "*Cybersecurity - Challenges and perspectives in education*"[3] coordinated by RAISA.

[1] C. Ciuchi, I.C. Mihai, G. Petrică a.o., Cybersecurity guide, 2021, ISBN 978-973-0-33645-0, electronic edition, DOI: 10.19107/CYBERSEC.2021.EN

[2] G. Petrică, S.D. Axinte, I.C. Bacivarov, Dependability of information systems, Matrix Rom, 2019, ISBN 978-606-25-0529-5

[3] I.C. Mihai, C. Ciuchi, G. Petrică (editors), Cybersecurity - Challenges and perspectives in education, Academica Greifswald, 2020, ISBN 978-3-940237-26-2, DOI: 10.19107/CYBERSEC-EDU.2020.EN

- Participation of RAISA specialists - as professors - in some courses within the master programs in the field of dependability and cybersecurity, held at technical and economic universities. We mention in particular the courses held within the master's program "*Quality and Dependability in Electronics and Telecommunications*" - ICSFET from Faculty of Electronics, Telecommunications and Information Technology - Politehnica University of Bucharest.
- Organization of several *RAISA workshops*, dedicated especially to young researchers, engineers, MSc and PhD students in IT field (especially in cybersecurity), who analyzed the challenges and implications in the field of cybersecurity, in the context of the crisis generated by the coronavirus.

References

[1]. https://www.un.org/development/desa/dspd/everyone-included-covid-19.html (accessed May 1st, 2021).

[2]. https://wellcome.org/news/equality-global-poverty-how-covid-19-affecting-societies-and-economies (accessed May 10th, 2021).

[3]. https://en.wikipedia.org/wiki/Social_impact_of_the_COVID-19_pandemic (accessed May 15, 2021).

[4]. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (accessed May 15th, 2021).

[5]. https://www.kaspersky.com/blog/pandemic-year-in-infosec/39123/ (accessed May 15th, 2021).

[6]. https://securityintelligence.com/articles/how-to-create-a-cybersecurity-framework/ (accessed May 20th, 2021).

[7]. https://orangecyberdefense.com/global/white-papers/covid-19-a-biological-hazard-goes-digital/ (accessed May 20th, 2021).

[8]. I. Bacivarov, Editorial: RAISA and IJISC - 5 Years in the Service of Cybersecurity Culture Dissemination, International Journal of Information Security and Cybercrime, vol. 6 (2017), no. 1, pp. 9-12.