10.53477/2668-2028-21-38

THE EFFECT OF COVID-19 EPIDEMIC ON DIGITALIZATION

Adriana-Meda UDROIU, PhD
National Institute for Research and Development in Informatics
meda.udroiu@rotld.ro

Ionuț SANDU
National Institute for Research and Development in Informatics
ionut.sandu@rotld.ro

Abstract: *When the COVID-19 epidemic hit Europe at the end of February 2020, most countries enforced a lock down period. In terms of public services, that means that citizens could rely only on digital services provided by the Government or local authorities. In countries with a low level of digitalization, the lock down generated a freeze of some public sectors. One of those countries was Romania, which since March 2020 has had a mixed approach to the bureaucratic challenges that were brought by COVID-19 global pandemic. In March 2020, with an almost nonexistent and underdeveloped digital infrastructure, Romania could only take emergency measure in terms of public services. More precisely, all non-urgent services were frozen or postponed while the validity date of official documents (e.g. medical certificates, identity cards) was extended. Starting with May, some public institution managed to provide some sort of digital services, though most of them do not comply with the data protection regulations.*

Keywords: *COVID-19 epidemic; digitalization; pandemic context.*

Introduction

The Coronavirus pandemic has brought record-breaking unemployment level, millions of shuttered businesses, cancellation or postponement of sporting events, numerous deaths and infections. We are limiting real life interactions and outdoor activities as much as we can. Everyone's obvious first priority is to stay safe, stay afloat, and get through this crisis. In Romania, schools are remote, universities are remote, people can get a medical check-ul remotely, order food remotely, and even courses like dancing can be taken remotely. Organizations are coming up with plans on what to do right now, and what to do long-term. Cutting costs and firing employees, might help the companies with short term cash, but in the end, the most important initiative for most companies is represented by the digital transformation. There has been a huge uptick in the use of digital technologies that help reduce face-to-face interactions. Still, people need to leave their homes more often that they should.

Excluding the common needs, emergencies, and non-diagonalizable actions, the majority of the cases where people had needed to leave their homes was because of bureaucracy. Since February 2020, I had to leave my home multiple times, and I think that if Romania had better digitalization, some of those times would be replaced with a few clicks. Some personal examples: requesting expired national ID change, signing university study contract, picking up student ID, changing my general practitioner medic, etc. Have some digital alternatives been available, I would have for sure choose them, not only because they seem faster for me, but also because of the pandemic context. If COVID-19 would have not been a thing, would I still choose the digital way? Probably yes, because while there are also downsides of digitalization, in my opinion, the advantages far outweigh the disadvantages.

Advantages and disadvantages

During pandemic times, the biggest advantage is also the most obvious one: less face-to-face interaction. According to World Health Organization, COVID-19 is caused by the SARS-CoV-2 virus, which spreads between people, mainly when an infected person is in close contact with another person. It is evident that, by lowering close physical contact between persons, we can also lower the rate of SARS-CoV-2 infections. Another advantage of digitalization is, in my opinion, the speed of the operations. First of all, there is no need for someone to get ready to leave home and

physically go to the institute, which cuts the commuting time. Second of all, requests done online are done faster. Ordering a pizza? Why not clicking the "Reorder" button on your last order? Lastly, requests done online might be and fulfilled faster, because searching in a digital database is way faster than searching in a physical one. Yet another advantage of digitalization is the cost efficiency. Printing, shipping, renting physical space costs companies lots, costs which can be avoided by going digital. Enhanced Information preservation is another advantage of digitalization. Handling information stored in paper formats degrades with each use, while opening a digital document does not degrade it regarding of the number of times its opened. The risk of a disaster is always present. A destructive phenomenon may cause loss of paper documents. Good digitalization comes with backups, which can be used for disaster recovery. Less commuting, less printing, less physical documents, all contribute to another advantage of the digital transformation, which is that it is environment friendly.

Providing a fast and efficient service is not cheap. Even less so if we are talking about countywide digitalization, such as Estonia's case. The first disadvantage, in my opinion, is represented by the initial cost of making the switch from physical to digital. To be digitalized, a service must provide not only confidentiality, integrity and availability, but also transparency and data ownership. Protecting data from cyber-attacks is a much harder task than protecting physical data. That is why, with digitalization, there are also risks, such as the risk of the sensitive data being accessed by unauthorized persons, etc. This represents the second disadvantage of going digital. However, if done properly and with enough resources, a system which provides all of the above can be achieved. Social disconnect, social depersonalization and addiction can also represent disadvantages and risks of digitalization. However, every tool can be dangerous if used incorrectly or for long periods of time. Digitalization might make the human factor feel less important, but it is up to each individual to spend their digital time thoughtfully.

Use case: Romania

Generally, Romania has three approaches for public services management during COVID-19 pandemic:

A. Institutions that still rely on paper work, e.g. Directorate for persons record and databases management.

These institutions could not find a digital solution and citizens still need to interact with a human or make a request in person. Citizens need to make an appointment and wait for a free slot to have their request handled. In case of an emergency state, these institutions close their activity or only handle the emergency cases.

B. Institutions that can receive and handle services digitally, e.g. General Directorate of Social Assistance and Child Protection

Some institutions implemented online procedures for their services. Most commonly, the citizens must send the required documents by email, they can make an appointment to have a video call with the civil servants when needed, and they receive the papers back by post or email. Although these online procedures can address most requests of the citizens, they do not provide the required level of data security, since the institution had not had resources to implement the digital services properly.

C. Hybrid services, e.g. universities, private companies

These are the cases when digitalization is implemented to the limit of legal coverage: e.g. documents signed digitally have no legal value. Only digital signature (with a certificate attached) is recognized, but there very few citizens who own such signatures.

Thought the status of digitalization in Romania is uncertain and chaotic, there are a number of advantages (especially for the citizens), as well as disadvantages of the systems implemented in the context of the 2020 pandemic, such as:

- restart of the social system: the public services related medical and disability care were among the first ones to implement digital procedures. Thought they are not secure, it was more important for them to function;

- digitalization proved that many bureaucratic procedures are unnecessary, most of the legal affairs could to be managed without too much paperwork or human intervention;
- digital management of public services is faster and safer in terms of public and personal health;
- digitalization provides less space for fraud and corruption of civil servants.

But there are some disadvantages, such as:

- most digital procedures implemented during pandemic are not secure;
- lack of standardization;
- unfeasible for long term usage, since the digital solutions were not based on a solid digital infrastructure;
- lack of legal coverage.

While this kind of hybrid, emergency digitalization procedures help some public institution resume their activity, it is far from the solid and secure form of digitalization used by Estonia. The COVID-19 pandemic emphasized the need for digital public services, but Romania should start building them according to the legal standards.

Cyber attacks

Cyber-attacks happen all the time, regardless of the world being in a pandemic or not. Cybersecurity problems concern not only large entities like tech companies or banks, but also smaller companies with less employees, going down to each individual. There concerns grew during the pandemic time, because of reasons which mostly have to do with the fact that people work and spend more time at home.

The pandemic caused a large number of people to start working from home. While cutting commute times and working from the comfort of their homes might be an advantage for others, spending more time at home can represent a huge cybersecurity risk. There are multiple reasons behind this, some of them being enumerated below.

- The home networks are less secure than the office networks. This happens because companies hire people dedicated to securing the office network, while home networks are being secured by each individual, and mostly consist of setting up a Wi-Fi password.
- Taking the work laptops out of the office represents a risk because it is easier for someone with malicious intents to steal them and then attain sensitive information.
- It caused people to shop more online, order food and generally be more digitally connected than ever.

The FBI reported that the number of cyberattacks is up to as many as 4,000 a day. This represents a 400% from what they were seeing pre-coronavirus[1]. Interpol is also seeing an "alarming rate of cyberattacks aimed at major corporations, governments, and critical infrastructure"[2]. Microsoft reports that COVID-19 themed attacks, such as phishing or social engineering attacks have jumped to 20,000 to 30,000 a day in the U. S[3]. The F5 Security Incident Response Team reported that, even if the year 2020 started with the number of incidents in January at half of the average reported in previous years, the reported incidents rose sharply as the pandemic shelter-in-place took effect in March[4]. Over the period of January

[1]https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus pandemic

[2]https://abcnews.go.com/Politics/alarming-rate-cyberattacks-aimed-major-corporations-governments critical/story?id=72164931

[3] https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-duringthe-outbreak/

[4] https://www.f5.com/labs/articles/threat-intelligence/how-cyber-attacks-changed-during-the-pandemic

through August, 45% of reported security incidents were DDoS, 43% were password login attacks and 12% were malware infections, web attacks or were unclassified.

Warren Buffett once said, "Don't let a good crisis go to waste." Cyber-attackers have long subscribed to this mantra, and it's clear from the past few months that they are continuing to follow this approach.

The Seven Phases of a Cyber-Attack

The first one is Reconnaissance, where the attackers get to know the target. They find out who are the important people in the company, who they do business with, what public data is available about the company. The second one is Weaponization, where the hackers use the information that they gathered in the previous phase to create the things they will need to get into the network. The third step represents the Delivery. The fourth one is Exploitation, where the attackers use information from the delivered payload to gain access or information. The fifth step represents the Installation, in which the attackers make sure that they have continuous access to the network. The second to last step is Command and Control, where they can impersonate users, lock systems and basically control the network. The final step represents the Action on Objective, in which they can steal information, designs, they can mess with operations of the company.

WHO Reports Fivefold Increase in Cyber-Attacks

Since the start of the COVID-19 pandemic, WHO has seen a dramatic increase in the number of cyberattacks directed at its staff[5]. On 23 April 2020, WHO reported that more than 450 active email and passwords were leaked.

Scammers impersonating WHO in emails have also increasingly targeted the general public in order to channel donations to a fictitious fund and not the authentic COVID-19 Solidary Response Fund.

In response to the attacks, WHO started working with the private sector, to establish more robust internal systems, to strengthen security measures, and educate the staff more on cybersecurity risks.

CERT reports phishing campaign which uses the image of the World Bank

On 28 April 2020, CERT reported a special tailored website for phishing attacks was operating on Weebly platform[6]. CERT states that, because Weebly is a free platform, it is often abused by attackers for hosting malicious content and launch attacks. This phishing campaign copies visual identity elements of the World Bank, with the purpose of making the users enter their bank details into the website.

The website used an automated translate tool for the text, and because of that, the text was not coherent. However, the attackers bet on the sense of urgency, trying to convince the victim to enter his bank details in order for his accounts to not be blocked.

The bank details that the victim was asked to enter were: name, IBAN, email, internet banking ID and the password generated by the token. With this information, attackers would be able to gain access and make transactions from the victim's bank account.

SIM Swap Fraud

SIM swap scams (also known as 'SIM-jacking') represents an cyberattack where an attacker hijacking a victim's mobile phone number by porting the number to a SIM card that's under their control. Since users are often authenticated with a one-time passcode sent to their

[5] https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
[6] https://cert.ro/citeste/alerta-phishing-banca-mondiala

phone number, criminals can use data obtained from darknet or social media feeds to compromise email, bank or online accounts.

In March 2020, Europol issued a warning[6] that the SIM-jacking threat was growing across Europe. It revealing that an investigation had led to suspects linked to the theft of more than $3.8 million.

The Phases of a SIM Swap Attack

1. *Reconnaissance* – identifying a victim and their mobile number, collecting personal information from dark web, social media feeds or phishing emails.
2. *Weaponization* – attackers come up with a method to use the gathered data to trick the victim's mobile carrier into transferring the victim's phone number to their own SIM.
3. *Delivery* – attackers trick the victim's mobile carrier into transferring the victim's phone number to their own SIM. This can be done remotely or even in store.
4. *Exploitation & Action* – attackers use the victim's mobile number as a form of 2FA to reset passwords and access their online accounts.

Conclusion

Digitalization is faster and more efficient than traditional ways and, during the pandemic times, it reduces close contact between persons. However, digitalization is a tool and it is not here to replace human interaction. It is up to each one of us to not lose ourselves in the digital world.

Acknowledgements

This research work was financially supported by a grant awarded by the Romanian Ministry of Innovation and Research, UEFISCDI, project number 8SOL/2018 within PNCDIII, project code: PNIII-P2-2.1-SOL-2017-09-0102, project name: Integrated Information System for Management of Activities (IISMA) (http://sima.ici.ro/en/).

BIBLIOGRAPHY

1. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronaviruspandemic
2. https://abcnews.go.com/Politics/alarming-rate-cyberattacks-aimed-major-corporations-governmentscritical/story?id=72164931
3. https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-duringthe-outbreak/
4. https://www.f5.com/labs/articles/threat-intelligence/how-cyber-attacks-changed-during-the-pandemic
5. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
6. https://cert.ro/citeste/alerta-phishing-banca-mondiala
7. https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millionshighjacking-phone-numbers

[6] https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millionshigh jacking-phone-numbers