THE
Fine
PRINT

Gökçe

March 2019
78

NEW CULTURE OF THE DIGITAL AGE: CYBERSECURITY

Highlights of this issue

Interview with Mehmet Bedii Kaya, PhD

NEW CULTURE OF THE DIGITAL AGE: CYBERSECURITY

One of the most valuable things in our era is to reach any information quickly and easily. Technology is evolving around this purpose and try to make it better. Therefore, technological tools are being used more frequently by public and private entities and as a matter of fact are integrated into their organizations. In this context, numerous public institutions and organizations are trying to be more "technologized". Turkey Statistical Institute's (TSI) 2018 Household Information Technology Usage Survey shows us the increase of computer and internet usage among 16-74 aged individuals' comparing 2017 data; computer use has increased to 59.6% and the use of the Internet has risen to 72.9% [1]. Another TSI's survey, 2018 Information Technology Usage Survey in Enterprises, shows that the internet access rate of enterprises having 10 or more employees is up to 95.3%[2].

Information and communication technologies are not just involved in the private sector but also highly integrated into the relations of the individuals with public institutions and organizations. In this context, the "e-government" system may be shown as the most comprehensive example. By means of this system, citizens are able to request the public documents via online systems and make many applications via the same. Again, the electronic notification system and the registered electronic mail which have been on the agenda for a long time in recent years are some of the essential examples of the efforts made by the public institutions and organizations to follow the technology.

The abovementioned examples are just some of the efforts to keep up with technology. Since computers and electronic devices have rapidly involved in our lives over the years, protecting our private life in the field of information technologies become a necessity. The widespread use of technologies and the establishment of information based economy have made cybersecurity and data privacy risks more and more spoken. This is where the concept of cybersecurity comes to the fore:

What is the meaning of cybersecurity?

The National Cyber Security Strategy texts prepared by the Ministry of Transport and Infrastructure define cybersecurity as **protection of information systems that make up the cyber space from attacks, ensuring the confidentiality, integrity and accessibility of the information being processed in this space, detection of attacks and cyber security incidents, putting into force the countermeasures against these incidents and then putting these systems back to their states previous to the cyber security incident.**[3] Accordingly, cybersecurity might be briefly explained as protecting the cyberspace from end to end, particularly the information systems and the security and confidentiality of the data contained in these systems.

According to the above definition, cyber security does not merely elaborate the security of public institutions and organizations or individuals in the cyberspace; it is an umbrella concept covering all aspects. Thus, the reflections of cybersecurity on the lives of individuals may be protection of their personal data but, with respect to companies or administration, it may be information security and operational security. However, this does not mean that cybersecurity has limited perspectives. Even if cybersecurity is related to data security and is generally elaborated within the scope of personal data protection, evaluating cybersecurity only in this context will reduce the importance of the matter.

[1] http://www.tuik.gov.tr/PreHaberBultenleri.do?id=27819
[2] http://www.tuik.gov.tr/PreHaberBultenleri.do?id=27820
[3] http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf

The inconveniences arising from cybersecurity gaps for private sector actors are not just limited to data breach. There might be also loss of trust of customers and business partners, loss of capital, competitiveness and reputation, facing administrative penalties and indemnity claims. The private sector actors who are aware of the value of cybersecurity give special importance to cybersecurity while using information and communication technologies, try to identify the existing gaps, cure them, make detailed and regular reporting, keep their systems up to date, back up their data and take necessary policies and measures. In addition, whilst the system gets wider and wider, the measures to be taken should increase as well.

Therefore, many companies now apply to cyber insurances in order to prevent losses that may be caused due to cybersecurity gaps and they have become the shelter of many companies.

Cybersecurity Regulations

One of the most important legal developments in recent years is the enactment of the Cybersecurity Act approved by the European Parliament. Henceforward, the European Network and Information Security Agency (ENISA), which acts as an independent expert body, has been made permanent and provided with more financial resources to achieve cybersecurity objectives. In addition, the cybersecurity certification system for goods, services and transactions circulating across the European Union is established.

Although such a regulation on cyber security exists in the EU; Turkey does not have a specific and separate cybersecurity regulation. In this context, the main regulations related to cybersecurity in our country consist of the Law no. 5809 on Electronic Communication Law and the Council of Ministers' Decree on the Implementation, Management and Coordination of National Cyber Security Studies dated 2012. Within the scope of these regulations, the Cyber Security Council has been established and numerous duties of cybersecurity are undertaken by the Information and Communication Technologies Authority. The Law on Personal Data Protection may also be considered as another regulation regarding cybersecurity. It is understood from the explanations and action plan that this matter is intended to be regulated as soon as possible.

It should be noted that in parallel with the technological developments, information security and operational security issues become more and more vulnerable to violations and open to the gaps. Cybersecurity experts point out new challenges that we may face in 2019. Some of these challenges are critical infrastructure security, machine learning and artificial intelligence in cyberattacks and IoT risks. Therefore, it is crucial for companies to secure their systems as quickly as possible; put into their agenda certification processes such as ISO 27001 as a control mechanism and try to eliminate risks by identifying them initially. We hope that these predictions will not be happening. However, the right approach for everyone who is in contact with technology would be to give greater importance to cybersecurity and take the appropriate measures considering possible damages and losses.

For further information please contact us at contact@gokce.av.tr

INTERVIEW WITH MEHMET BEDII KAYA, PhD

We discussed with Mehmet Bedii Kaya, PhD, who is an academician in Istanbul Bilgi University Information Technology Law Institute, about cybersecurity. You may find our pleasant interview below with Mr. Kaya having intensive studies on cybersecurity both in European and Turkish legal circles.

1. How do you explain cybersecurity to those who are not familiar with cybersecurity?

Cybersecurity includes various layers and aspects. Therefore, it is not always easy to explain cybersecurity in a simple and easy way. To explain it better, we may contribute to the matter with a little analogy. Just as we pay attention to our physical and domestic security as part of our personal security, we should also pay due attention to our cybersecurity. In this context, we can define cybersecurity as paying attention to the security of all the information systems that we use and taking necessary measures at every level of the system.

2. How do you evaluate our society's perception of cybersecurity? Do you think our legislation meets the requirements?

It is difficult to say that there is adequate awareness in our society in relation to cybersecurity. Real persons or companies are only sensitive on cybersecurity matters, when they face a dispute or a problem or when a concrete damage occurs. Hence, we observe that companies are ignoring cybersecurity investments. Only after when they suffer from a real damage, they show proactivity.

Such perception does not mean that there are no obligations set forth in different legislations. It should be noted that even in a world where there are no legislations on cyber security, one of the most important liabilities of the companies is security as there are already bound by security obligations arising from contract law. All together, we realize that the matter is directly related to awareness rather than law. If we prioritize cybersecurity, make the necessary investments and thus contribute to the creation of awareness; we will reap the fruits of such awareness in various scopes, from company information and trade secrets to competition.

3. What do you think about cybersecurity awareness of public and private persons in Turkey?

Cybersecurity is a quite dynamic area required to show quick reflexes and keep up with the necessary updates. Therefore, although we hear about some projects and regulations, the public institutions fall behind and may not keep up with the pace of technological developments. I believe that the underlying reason behind this is our public administration perception. As I mentioned in the previous question, we see how limited the reactions of private persons and they view the matter from a narrow frame, unless there is a concrete breach and damage. At this point, we must emphasize that cyber security must be transformed into a company culture associated with reflexes and habits.

4. How should the relationship between cybersecurity, personal data protection and cybercrime be legally described?

In fact, the regulations on personal data protection have brought various obligations in relation to cybersecurity within the scope of information security. Turkey has made its breakthrough in the field of cybersecurity by means of the regulations of personal data protection and this issue has become much more dynamic. Thus, we may consider these regulations as a locomotive of the field. It should be noted that even if the compliance procedures for personal data are deemed to be completed, it does not mean that cybersecurity compliance is fully carried out. Cybersecurity requires a comprehensive perspective and therefore a comprehensive compliance procedure.

5. How did you find the Cybersecurity Act approved by the European Parliament? Do you think our legislation follows such developments in Europe?

We may consider that there is a precautionary adaptation process in Europe. Europe recently went through a directive enacted in 1995 on personal data to General Data Protection Regulation (GDPR), has been going through the same with the NIS Directive regarding infrastructures (Directive on Security of Network and Information Systems) and the Cybersecurity Act. In parallel, Turkey is closely following these developments. The enactment of a separate cybersecurity law is also mentioned in the political goals of the Information Society Strategies documents. The important thing is that these regulations should always be enacted with participatory democratic methods and should foresee a gradual transition period due to the special conditions of Turkey. Hence, the necessity of designing such a system should not be overlooked.

6. In your opinion, what kind of cybersecurity threats we will see in the near future?

Cybersecurity threats are constantly evolving and hybrid actors appear rather than sterile cyber world actors. Let's give the example of a gray hat hacker. Recently, a gray hat hacker in Europe mended a security flaw by entering into information systems and made thousands of them more secure. It may sound a bit weird, but he/she is well-meant. However, at the end of the day he/she still breached the relevant information systems. On the other hand, ransomwares also reached different levels. The hackers who possess the files by using one of the recent ransomwares, demanded to exceed 100 million likes of a video on their YouTube page to release the files. When this number is reached, the ransom software frees the files by means of automatic bot.

We observe each day new threats, new generation criminals, new generation Robin Hoods, challenges and ego wars in cybersecurity field. One of the methods of hacking called phishing has now been replaced by another method called spear phishing. In phishing, the net is casted in general and those who fall into the net suffer from the cyberattack. However, a specific sector is targeted and cyberattack is aimed at the sector in spear phishing. For example, Turkish companies' accounting departments in industry sector receiving and rendering payments are occasionally targeted. The accounts of these companies are manipulated by spear phishing and their payments are directed to different channels or in some way their managers are targeted. Such situations may bring together the organizations, units or structures, not possible to come together in our opinion, and ensure the unity of the purpose and business. In brief, threats are evolving every day and they become more personalized rather than being general.

THE Fine PRINT
Gökçe
March 2019
78

Answers. Not theories.

Gokce Attorney Partnership

Editors:

Assoc. Prof. Dr. Ali Paslı
ali.pasli@gokce.av.tr

Bahadır Bektaş
bahadir.bektas@gokce.av.tr

Dila Erol
dila.erol@gokce.av.tr

Yağmur Yollu
yagmur.yollu@gokce.av.tr

Ahmet Başaran
ahmet.basaran@gokce.av.tr

Fatih Ermiş
fatih.ermis@gokce.av.tr

About our firm

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at
contact@gokce.av.tr
0 212 352 88 33

The Fine Print is prepared and published for general informative purposes only and does not constitute legal advice or create an attorney-client relationship. Should you wish to recevie further information, please contact Gokce Attorney Partnership. No content provided in The Fine Print can be reproduced or re-published without proper attribution or the express written permission of Gokce Attorney Partnership. While all efforts have been made to ensure the accuracy of the content, Gokce Attorney Partnership does not guarantee such accuracy and cannot be held liable for any errors in or reliance upon this information. The Fine Print was created for clients of Gokce Attorney Partnership and the possibility of circulation beyond the firm's clientele should not be construed as advertisement.

For further information please contact us at contact@gokce.av.tr