DOI: 10.17951/rh.2019.47.355-359

New Challenges in Records Management? Thoughts on Marvin Waschke's, *Personal Cybersecurity. How to Avoid and Cope with Cybercrime*, Apress, New York 2017, pp. 240.

Marvin Waschke is a well-known American computer system architect working for large companies, banks and government institutions. For many years he has been analysing contemporary computer systems and networks, including those utilising cloud storage technologies[1]. He is an author of a series of publications on the matter, among the most recognised works are: *How Clouds Hold IT Together: Integrating Architecture with Cloud Deployment* (Apress, New York 2015) and *Cloud Standards: Agreements That Hold Together Clouds* (Apress, New York 2012).

The author is both a theoretician and a practitioner who faces cybersecurity issues daily. The goal of the reviewed book is to compile major problems associated with management of security systems in a large national institution and private companies, analyse them in detail and demonstrate to avoid general threats which involve modern IT solutions.

As highlighted by the author, for many years the creators of IT management systems and programmers neglected data security in some areas. They just did not give it much thought. However, the rapid rate at which information technology is being developed and consequently, a new type of criminal activity, cybercrime[2], changed the approach to this issue. As he pointed out, the threat becomes higher with every new electronic device in use, each new application or software that is installed on them[3].

---

[1] In spite of the concerns, cloud data storage remains safe and the volume of files we keep in the cloud increases, trusting in the security measures employed by third parties, e.g. Google; more about storage safety can be found at i.a. https://bitdefender.pl/przechowywanie-danych-w-chmurze-nadal-jest-bezpieczne/ [access: 10 VI 2019].

[2] The definition of cybercrime was explored by i.a.: J. Bednarek, A. Andrzejewska, *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Warszawa 2014, M. Siwicki, *Cyberprzestępczość,* Warszawa 2013, J. Kosiński, *Paradygmaty cyberprzestępczości,* Warszawa 2015, P. Wiśniewski, J. Boehlke, *Cyberprzestępczość w gospodarce,* Toruń 2016.

[3] Further information on mobile software installation can be found in i.a. D. Chell, T. Erasmus, S. Colley, O. Whitehouse, *The Mobile Application Hacker's Handbook*, Indianapolis 2015.

He emphasises that an increasingly common occurrence among cybercriminals is the surprisingly dangerous practice of stealing personal data[4], which is then used for marketing or in criminal activity. Such crimes are more common than unauthorised access to bank accounts or financial scams. As he points out, the profile of persons who breach information systems and personal computers is dynamically changing. Three main groups can be distinguished among them. The first are the 'white hat hackers' who test the security of specific information systems with the consent of the administrator, the second is the 'grey hat hackers' who act without consent, but they mean well as they wish to uncover malpractice of entrepreneurships, government officials or politicians, and finally, the 'black hat hackers' who specialise in illegal activities. According to Mavin Waschke, the most dangerous at the moment are criminal groups specialising in compromising computer networks, which are often a part of mafia structures. Sometimes they work for companies that wish to discover the plans of the competition or steal technical data of their products. These activities frequently involve the participation of countries such as Russia, China, North Korea or the so-called 'Islamic State'. These special units operating for countries inside the cyberspace are considered as one of the largest current threats.

In the book a new phenomenon was described which increased in intensity over the last few years, namely, hacking smartphones and tablets[5]. Clearly, it is a consequence of the cultural changes we have observed in recent decades. Mobile phones have long since evolved past a simple device for making phone calls and writing text messages. The dynamically growing number of available applications allows them to access online bank transaction services, handle official matters via appropriate internet platforms, shop online, etc.

Marvin Waschke highlights that a still relevant major issue is the lack of preparation of the administration, law enforcement to the new challenges and inadequate law and courts. Cybercrimes are often difficult to detect by IT specialists because the architecture of the internet makes it exceptionally difficult to determine the source of an attack. Another question in this context is whether these crimes should be prosecuted

[4] Since 25 May 2018 a regulation (EU) 2016/679 of 27 April 2016 of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repeal of directive 95/46/WE (general data protection regulation) (EU Journal of Laws, L series, No 119, p. 1 as amended).

[5] In Poland the phenomenon is described by websites involved in data security, i.a.: https://bezprawnik.pl/bezpieczenstwo-smartfona/ [access: 10 VI 2019].

in accordance with national or international law. As seen in practice, hacking attacks from abroad are committed increasingly often. Further issues involve moral and ethical assessment of hackers' activities which became visible especially in the context of WikiLeaks case.

An important advantage of the reviewed monograph is the emphasis on the relevance of securing data by public authorities, enterprises and entities. Breaches and theft of personal data and intellectual property are a constantly growing threat. Data security, and constant and quick access to it, became a challenge for leading companies that design and implement information security management systems. A growing wave of online criminal activity is proportional to the growing involvement of electronic devices in our daily routines. The aforementioned online bank transaction services, e-administration, e-documents are new instruments which are gaining popularity. Development of new technologies is so rapid that designers, engineers and administrators of new information security management systems cannot respond adequately quickly to new threats and seek support in updates which periodically remove security vulnerabilities. The larger the numbers of financial transactions and volume of accumulated and stored data on servers of various companies, the greater the pressure on the aforementioned persons to increase the security of new information security management systems which obviously involves increasing costs of operation. On the other hand, the growing online service market becomes increasingly more attractive to specialised cybercriminals or even cyberterrorists who use the funds obtained through online criminal activity for financing illegal criminal and terrorist organisations. The arms race between information security system developers and those interested in bypassing the safeguards is a constant work environment for people creating information security architecture. The pressure of time and increasing volume of stored data do not make it easy for specialists in the field.

Of course the aforementioned publication is not free from errors. Although it does precisely analyse and diagnose threats associated with the dynamic development of new information technologies, it mostly focuses on the technical aspect. It approaches the problem primarily from the point of view of computer system architects and administrators as well as information security management systems. It focuses on providing guidance for individuals and companies, advising on how to avoid harm from cybercriminals. Less attention was devoted to systemic solutions, human factor and social aspect. Currently the biggest problem is the fact that many websites or social networks utilise our personal data very skilfully in exchange for being able to use specific applications.

The very philosophy of social networks such as Facebook or Twitter facilitates such activities. The last scandal involving Face App is a clear example of such a threat.

It should be noted that the problem is currently not limited just to stealing credit card data or passwords to internet banking services or even personal data. Analysing our activity on social networks or on the internet in general is the latest trend used for profiling consumer, political and social preferences. The data can be used not just for preparation of a personalised marketing offer but can also constitute a key data source for political parties or even foreign authorities, which through a profiled propaganda message can to a certain degree shape voting preferences of inhabitants of a country, which, as we know, took place during the latest elections in the United States. That way they can influence specific political preferences, stir up xenophobic, separatist, anti-immigration or anti-EU attitudes. New information on conducting such activities by Russian services shows that dynamic development of information technology may facilitate attacks on the very foundation of liberal democracy.

Of course, we can hardly blame the author for not including all these issues in his monograph. This topic is very recent and keeps getting more and more complex. Therefore, in order to successfully prevent threats in virtual reality it is necessary to establish interdisciplinary teams comprising specialists of various fields, i.a. IT specialists, archivists, historians, lawyers, psychologists, sociologists, etc. We know that such teams are slowly being assembled in the largest countries, mostly in developed western democracies, which carry out actions with redoubled efforts to prevent these threats after the latest hacking attacks from i.a. China and the attempts of Russian services to affect the result of the voting process.

Also, data protection officers and archivists are faced with these new challenges because document management as an area of practice is becoming saturated with information and communication technologies. Therefore, it can be assumed that before conducting a scientific reflection in this field there is a need to address questions associated with cybersecurity, especially in relation to personal data protection, on a far broader scale than before.

The reviewed publication of Marvin Waschke constitutes a data source of a contemporary archivist, who is concerned not only with the traditional circulation of documents but also new technologies. In archive study programmes we can find not only subjects such as the history of chambers, administration or the judiciary system but also legal

foundations of document handling, as well as information security. In the near future we can likely expect further challenges and changes which will be a response to new phenomena observed in the work of an archivist or a data protection officer, who have to utilise the advancements of various scientific fields in order to provide a high level of safety in circulation and storage of documents.

Małgorzata Szabaciuk
(Maria Curie-Skłodowska University in Lublin)
https://orcid.org/0000-0002-2119-134X
malgorzata.szabaciuk@umcs.pl

REFERENCES

Legal Act

Regulation (EU) 2016/679 of 27 April 2016 of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repeal of directive 95/46/WE (general data protection regulation) (EU Journal of Laws, L series, No 119, p. 1 as amended).

Studies

Bednarek J. Andrzejewska A., *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Warszawa 2014.

Chell D., Erasmus T., Colley S., Whitehouse O, *The Mobile Application Hacker's Handbook*, Indianapolis 2015.

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Siwicki M., *Cyberprzestępczość*, Warszawa 2013.

Wiśniewski P., Boehlke J., *Cyberprzestępczość w gospodarce*, Toruń 2016.

Internet sources

https://bitdefender.pl/przechowywanie-danych-w-chmurze-nadal-jest-bezpieczne/ [access: 10 VI 2019].

https://bezprawnik.pl/bezpieczenstwo-smartfona/ [access: 10 VI 2019].