■ Chapter 1 ■

Challenges and Risks for the Securitizing of Information Data in Poland and the EU

Edward Jakubowski
University of Zielona Góra
Faculty of Economics and Management

Abstract: The progress of civilization with the development of technology is becoming more and more important in the context of the information threat. Threats to the security of information data are today crucial for the security of the state and society. Today, a serious challenge involves counteracting the threats to the security of information data in order to avoid the destabilization of information systems and ICT systems.
Keywords: security, information security, threat, information

Introduction

The 21st century is a rapid progress in civilization that has taken place in the area of technology and information. The main activities take place in the field of mobile and ICT technology through the public Internet, which has affected all spheres of human life. The rapid development of social networks, various types of communication media, as well as the development of large-scale online and mobile banking and e-government, contributed to easy and quick access to information. Information has become one of the most important resources of state organizations and institutions today.

The 21st century, in the literature of the subject called the information age, has brought about a change in the nature and shape of threats in the world, because in the times of universal access to information technologies, new dangers have arisen (Koziej, 2011, p. 268), which are closely related to the use of information networks and information systems, e.g. crimes using a computer as a tool, loss of information related to computer hacks, malicious codes and viruses, espionage, sabotage, vandalism (Liderman, 2012, p. 24).

The growing role of information in the modern world increases the threat to its security (Nowak, Scheffs, 2010, p. 22).

The purpose of the paper is to present the challenges and threats to the security of information data in Poland and the EU in the era of open access to the Internet.

Information security

Information security is, in the most general sense of this wording, the storage of information in databases which should be protected. This applies in particular to data of a strategic nature, of key importance for the functioning of the enterprise, or another entity, or an ordinary person. The project referring to the information system supporting strategic management, should take into account the issues related to information security, by defining a whole set of rules as well as the methods and tools for protection, as well as the supervision over information. The definition of information security is very problematic, because the technological development in the field of computerization is changing intensively, there are more and more new activities that break the protection. Thus, the precisely formulated definition is closely related to the term referring to the security attribute to which it belongs in the literature:

a) confidentiality – information for unauthorized persons, entities or processes is not available,
b) authenticity – the identity of a particular entity or team is as it was previously declared,
c) accessibility – the opportunity to use on the part of a person who has the right to do so, at a particular time,
d) data integrity – an indicated quality means that certain data has not been changed or destroyed in an unauthorized manner,
e) system integrity – a quality that allows the system to perform the previously intended function in an unaffected manner by unauthorized manipulations (intentional or accidental),
f) integrity – data integrity as well as the system,
g) accountability – the activities of a particular entity, for example a user, may be assigned to them,
h) reliability – consistent as well as intended behaviour and effects (Czekaj, 2012, p. 128).

Information security can be understood as a resultant of legal security as well as physical, information and communication (ICT), and personal-organizational security (Polaczek, 2006, p. 137).

Security measures are taken during situations that pose a threat to the system or resources due to the fact that they are difficult and very costly tasks, as a result of which they are often interrupted or not applied at all. More and more threats are encountered in the modern world, which at the same time increases the risk of violating the protection of data collection and use as well as information loss. Therefore, it is necessary to create a strategy model for information management and its security in the organization, which includes such elements as: systems, processes, people as well as processed information (Czekaj, 2012, p. 129).

Threats to information security

In the modern world, information is an extremely important "commodity", which is why it is often an element of criminal activity aimed at obtaining it in an illegal and unauthorized manner. The first threat in this regard is cybercrime.

The concept of cyberspace is often used as a synonym for the Internet or for all activities related to the use of a computer, computer system, computer networks or any electronic communication system (Siwicki, 2013, p. 15). It is also indicated that the most accurate is to understand cyberspace as a "digital space for processing and information exchange processed by ICT systems and networks, along with links between them and relations with users" (Szpor 2011, p. 357).

According to the definition developed during the 10th United Nations Congress on the Prevention of Crime and Treatment of Offenders, a division was proposed for:

1) cybercrime in a narrow sense (computer crime) involving attacks against the security of computer systems and electronically processed data, committed with the use of electronic operations;
2) cybercrime in a broad sense (computer crime) covers acts committed with or against a computer system or a computer network, such as illegal possession and the sharing or dissemination of information via a computer or a network (Siwicki, 2013, p. 16).

The term cybercrime is used by the Commission of the European Communities, which in the Communication from the Commission to the European Parliament, the Council and the Committee of the Regions from 2007 on "Towards a general strategy to combat cybercrime" under this term means "criminal acts committed using electronic communications networks and information systems or directed against such networks and systems". Cybercrime consists of three types of attacks. The first includes "traditional" forms of crime, such as fraud or falsification committed using electronic information networks and information systems. The second type is the publication of illegal content in electronic media (e.g. materials related to the sexual abuse of children or incitement to racial hatred). The third type includes crimes typical of electronic communication networks, e.g. attacks against information systems, DoS attacks and IT sabotage. The Communication also indicates that all these types of crimes are connected with the fact that they can be committed on a mass scale, and a geographical distance between the place of committing a crime and its consequences can be significant (Siwicki, 2013, pp. 16-17).

In general, a group of acts, known as cybercrime, includes the use of telecommunications networks (e.g. a public switched telephone network (PSTN), a computer network, the Internet, a telex network, a digital service integration network – ISDN) to violate any legal good protected by criminal law. The most important features of cybercrime can be considered as acting in a specific environment genetically related to computer technology and using it to commit common crimes (e.g. fraud, document falsification) as well as less conventional ones (e.g. cracking, hacking, phishing). The cybercrime includes:

1) offenses against the security of information being processed,
2) crimes related to the use of mass media to disseminate or present information prohibited by law (so-called offenses related to the content of information),
3) other crimes involving the instrumental exploitation (use) of electronic information networks and information systems to infringe legal goods protected by criminal law (Siwicki, 2012, p. 246).

Information security very broadly refers primarily to issues related to electronic banking. The issue of security in the area of internet banking is considered in the recommendation of the Polish Financial Supervision Authority of November 2015 relating to the security of payment transactions executed via the Internet by banks, domestic payment institutions, domestic

electronic money institutions and cooperative savings and credit unions. This document indicates a number of recommendations, including organizational and technological solutions aimed at increasing the security of access to online banking services. The Polish Financial Supervision Authority indicates recommendations in the area of data authentication, duration of single sign-on sessions, application of a strong authentication procedure involving the use of three independent elements, of which at least two are associated with the client. Undoubtedly, the content of the recommendation is closer to banking practice than fairly general regulations of the statutory rank (Rutkowska-Tomaszewska, 2017, p. 141).

Threats that are associated with the use of e-banking were primarily presented by the Polish Financial Supervision Authority. The Commission first of all listed them as:

a) phishing of data that allows transactions to be carried out;
b) theft with the use of malicious software for this purpose;
c) copying the payment card;
d) theft using a card with the possibility of contactless payments;
e) theft using data from the payment card customer;
f) dangers that are associated with the use of mobile applications;
g) customer identity theft;
h) "Nigerian fraud";
i) theft in the online store (Polish Financial Supervision Authority, 2014, p. 11).

The Polish Financial Supervision Authority also lists crimes related to e-banking, which have their regulations in Polish law. These crimes include:

a) Hacking, that is obtaining unauthorized access to all data by breaking security systems.
b) Spoofing, which should be understood as taking control of computers that belong to other users of electronic banking, which is intended to be used for activities that go beyond the relevant legal norms.
c) Sniffing – capturing information transmitted in local networks and WiFi networks, which is aimed at obtaining data of bank clients for their subsequent unlawful use.
d) Installing devices on ATMs that collect data from a payment card.
e) A computer virus, a program that has been placed in another program that replicates itself. As a result of this type of virus, for example, it is

possible to lose important data from the computer or to have difficult work in practice.

f) Puzzle bomb – a kind of virus. Its activation takes place on a specific day as well as at a specific time, and as a result of the user's execution of a particular operation.
g) Computer worm – the indicated type does not destroy data, but it may lead to loading of some programs on the computer.
h) Trojan horses, commonly known as so-called "Trojans". They can capture, for example, access passwords from the user of a particular computer. They start when a specific computer program begins.
i) Phishing – its essence consists in sending by e-mail messages from people who impersonate a particular bank, for example with a request to log in to the bank's website – these actions are aimed at phishing individual data about the client (such as password).
j) Pharming – is a form of phishing. It involves redirecting the user of e-banking from the correct bank website to the one that was created in order to scam individual data from the client (Polish Financial Supervision Authority, 2014, p. 11).

ICT security covers in this context all actions that should be taken to guarantee a defined level in ICT systems:

a) Confidentiality;
b) Integrity;
c) Accessibility;
d) Accountability;
e) Authenticity;
f) Reliability (Grzywak, 2003, p. 207).

One of the most important issues related to the functioning of ICT systems is the identification of users. It is most often implemented using a third, trusted website that meets the organizational and technological requirements as set out by law. In the case of electronic communication used most commonly in practice, the solution is an electronic key certified by designated institutions (Gołaczyński, 2016, p. 175).

Attacks that used malicious financial software in 2013 concerned 66,74% of malicious banking programs, 4,18% of *keyloggers,* 20,18% of software that stole *bitcoin* portfolios and software *downloaders* for *bitcoin* mining – 8,91% (www.securelist.pl, 29.04.2019).

Hacking attacks mainly concern financial frauds, which constitute up to 50% of attacks involving harmful software (Rutkowska-Tomaszewska, 2017, p. 129).

Mobile devices have not been a target for a long time from cybercriminals. Their first generations had limited functionality and it was difficult to create malware for them. The situation changed with the emergence of smartphones and tablets; devices having the direct opportunity to connect to the Internet as well as explicitly available tools for the development of applications. For several years, the number of malicious programs targeting mobile devices has increased, especially those with the installed Android operating system, which is vulnerable because it allows third parties to access *App Stores* and distribute rogue applications. Android is the main target of malicious attacks – in 2013 it represented 98,05% of attacks, which proves the popularity of the indicated operating system as well as the pressing issue of its software vulnerabilities (Rutkowska-Tomaszewska, 2017, p. 129).

In 2015, 2,333,777 new types of malware attacks were identified for devices with the installed Android system. Analysts from G Data SecurityLabs predict further increases in hacking attacks on smartphone and tablet users, as more and more people use mobile devices during *online* shopping or bank services. Experts from G Data underscore the fact that cybercriminals are targeting the Android system, and are generating significant profits.. Recently, criminals have been increasingly looking for gaps in systems that allow infecting cars connect to the Internet or electronic fitness bracelets. Most of them are controlled by Android applications (www.cyberdefence24.pl, 22.04.2019).

According to the prepared report "Kaspersky Security Bulletin 2015" in the ranking of the 10 most popular programs designed to steal money for the first time there were financial mobile threats, i.e. two groups of mobile banking Trojans (Faketoken and Marcher). Marcher programs steal data related to payments from Android devices. In turn, those from the Faketoken family cooperate with computer Trojans. The user is prompted to install the application on the phone, which is a Trojan that intercepts single-use codes confirming bank transactions (www.dobreprogramy.pl, 29.04.2019).

Research has revealed that 40% of applications do not check the authenticity of the SSL certificates used, which allows for the creation of a false certificate in order to perform a *Man in The Middle* attack. Over 20% of applications with the bank communicated without any encryption. As much as

90% of the application contained unencrypted links (without SSL), allowing a hacker (which from the application) to intercept the move, injecting the appropriate JavaScript/HTML code to create, for example, a false login screen to extract access data to the user's bank account. Over 50% of the applications are susceptible to embedded malicious JavaScript code due to the wrongly implemented user interface (UIWebView), in which entered and displayed information, among others allows for an XSS attack (for example allowing sending e-mail/MMS/SMS messages directly from the client device). Only 20% of the applications have launched PIE (*Position Independent Executable*) and *Stack Smashing Protection* options, reducing the manipulation risk that is associated with possible memory errors (www.niebezpiecznik.pl, 29.04.2019).

In the case of 70% of applications, there are solutions for confirming the identity of the bank's customer user, such as two-factor authentication, which, besides the password to access the account, also requires an SMS code sent by the bank. Moreover, static analysis has shown the possibility of extracting authentication data from the source code. The ease of acquiring such information enables hackers to gain access to the bank's development group and perform larger-scale operations, such as injecting malicious code into the application and infecting all clients logging in to the application using this application in this bank. Bank account information and customer transaction history can be extracted from the unencrypted *sqlite* database created by the application. The base can be captured remotely (by *exploit*) or locally, through an application that performs *jailbreak* of the iOS system (www.niebezpiecznik.pl, 29.04.2019).

The use of mobile banking involves the risk of losing confidential data as well as the possibility of unauthorized access to the bank's customer account. According to the 16th EY World Security Information Survey, the risk of using e-banking is growing. There are no safeguards on the market that cannot be broken. The mobile revolution is seen as the main threat to data security. According to EY, 83% of mobile applications allow hackers to break in and get data. Although the development of mobile banking is associated with an increase in risk, it is promoted as a banking solution arising from the the expectations of customers who want to make everything easier, simpler and faster. Unfortunately, such simplifications often occur at the expense of security. No security solutions can completely eliminate the risk (www.finanse.wp.pl, 29.04.2019).

Many millions of users can use the Internet at the same time. An important and still current problem in this respect is the issue of network security, especially in the context of the functioning and use of online banking, primarily in relation to providing the exclusive right of access to the account held to the client and managing the funds collected on it. The basic threats affecting the security of online banking have been relatively long identified, they include confidentiality and inviolability as regards the information provided, verification of the user's authenticity and access control (Juchno, Kaszubski, 2001, p. 12).

The key element for the online banking security is the possibility of the bank accepting the order that is made by the holder of a specific account - and not another person. An obvious difficulty in the indicated situation is the lack of simultaneous presence of the parties, at the same time affecting the inability to identify the direct identity issuing the disposition. The bank, as a service provider and also a public trust institution, has the responsibility to create solutions that enable effective the verification of a particular user's identity in order to ensure protection of the funds entrusted by clients (Rutkowska--Tomaszewska, 2017, p. 138).

In addition to the methods of committing crimes that are associated with the use of data, the literature has distinguished traditional physical methods of obtaining identification elements and methods related to the Internet. The first group included equipment theft, direct access to information, search of garbage, wallet theft, correspondence theft, reading over the shoulder, skimming, abuse by employees, telemarketing and fake telephones. The second group includes such behaviours as: hacking, phishing, pharming, redirectors, Nigerian fraud, keyloggers and password thieves (Lach, 2015, p. 159).

In this respect computer viruses are also very important. A computer virus is a self-replicating computer program placed in another program (the host). It has the ability to affect any element of the computer system. A computer worm is similar to a virus, but it makes its copies completely without a need for a host program. Computer worms also fill the computer's memory with a large amount of accidentally generated data, which causes the computer to slow down or cease functioning. A Trojan horse is software that pretends to be useful or interesting for the user, additionally has undesirable, hidden functionality. The effect of the Trojan horse may be, for example, the deletion of selected files, the formatting of the disk, the invoking of encryption

systems, and the sending of sensitive data to the author or owner of the Trojan horse. *Rootkit* is a hacker software that hides its presence in the system. It also allows hiding files, processes or network connections, so it can also hide the operation of other hacking programs. *Adware* is software that displays ads, in a negative sense it is software that tracks user activity on the Internet, and then creates its profile and displays contextual advertising. *Exploit* is a program or its fragment (usually a few lines of code) that exploits a vulnerability in the software installed on the victim's computer. *Dialer* is software that connects to the Internet through a different access number than the one chosen by the user. *Hoax* is a program that displays false information that a virus is on the computer (Plywaczewski, Filipkowski, Rau, 2015, pp. 531-532).

Ransomware is software that is spread mainly via email, but it is also possible to let it into the system through the actions of irresponsible users. Ransomware cuts off users from documents by encrypting files. By opening the attachment, the user initiates infection, software propagation, mutation and activation of system destructive functions. Malicious code downloads its updates, mutates and thus hinders its detection and retrieves the RSA key from the Internet. A step in encrypting files that are important to the user follows. Each of the files is encrypted with a separate key with a length of 256 bits, which hinders further process related to file recovery. The software is not limited to local file encryption; it searches network resources in order to extend the scale of the damage. The original files are removed from the user's local resources and from network resources. The documents are recovered only after paying the appropriate fee to the account of the software developer. The amounts vary from tens of dollars to several hundred thousand US dollars, depending on the wealth of the discredited organization (Kurpiewski, 2016, pp. 25-26).

Conclusion

Summarizing the above considerations, it should be pointed out that in the area of data security, the greatest threats are located in cyberspace. The studies on the multifaceted nature of cybersecurity lead to the conclusion that many countries around the world see the need to implement actions to ensuresecurity, and the problem is global. The analysis also shows that there are significant differences between individual countries in the area of legislation, organization and the technical means at their disposal to fight

cybercrime and attacks on systems and networks. Some countries have appointed special offices or agencies at government level which are responsible for technical or educational matters. Many countries have recognized the need for a strategy regarding cyber security as well as the establishment of incident response centres. A special role is also played by education pertaining to online threats; and many countries have assigned a special role to universities which conduct certified studies in the field of cyber security. Incidents that violate cybernetic security, either deliberate or accidental, the number of which is increasing at an alarming rate, may cause disruptions in the provision of basic services that are taken for granted, such as water supplies, health care services, electricity supply and mobile telephony services. The largest number of security incidents is related to the installation or use of unauthorized software in organizations, which represents a breach in that particular security system. The consequence of the bad security of IT systems and data processed in them may be criminal liability, the loss of reputation or financial loss.