Natalia Kondratenko
Department of International Business and Economic Theory
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
E-mail: ndkondratenko@karazin.ua
ORCID: https://orcid.org/0000-0003-2823-9905

Study of information security of the information services market

Abstract

The article is devoted to the study of information security of the information services market. *The subject* of the research is information security, and *the goal of the paper* is to study the information security of the information services market. Information security is considered a socio-economic challenge that can be addressed through the confident actions of the state. Data analysis confirmed the problem of information security at different levels. Information security is aimed at protecting information from unauthorized access. The development and transformation of the information services market depend on the quality metrics of the Internet. This paper deals with the issue of maintaining a sufficient level of information transparency, which is related to and interdependent on information security. The main risks and threats caused by the active introduction of information technologies and the advancement of the information services market are specified. The study found that in the day-to-day operations of each company, many risks can affect the information system due to information security breaches. Social engineering involves the use of psychological techniques to mislead users by providing information or access for attackers. In order for the company to cope with external risks in the information services market, it is necessary to build a strong risk management information system. The process of risk management is ongoing and iterative in nature, it must be repeated indefinitely as new threats and vulnerabilities emerge, especially external ones. The choice of countermeasures or controls used must strike a balance between productivity, cost, effectiveness, and the information value of the asset being protected. *Conclusions:* the research identified the basic principles of information security, namely confidentiality, integrity, and availability. Moreover, to increase the information security of the companies which are participants in the information services market, the author proposes implementing a range of measures within the company. Information security in the information services market is a marker of the crucial difference between the information society and the industrial society. The main hallmark of the information society is its openness. This means a significant reduction and thus a general lack of confidential information for society. The study established that the digitalization of the economy is modifying the information services market. The research findings may prove useful to businesses and governments to boost information security of the information services market. The research is based on the *methods* of theoretical generalization and comparison to define the concept of "information security" and its interrelations with other definitions of the relevant terminological framework. Analysis, synthesis, and scientific abstraction were used to identify factors affecting the risks and threats to information security of the information services market. There were used methods of analysis, comparison and generalization when summarizing research findings.

Keywords

information security,
information services market,
digitalization

JEL: A12, A13, D80

DOI: https://doi.org/10.30525/2500-946X/2021-2-20

1 Introduction

The onrush of scientific and technological progress and the global informatization of the world's developed countries play an important role in the current sweeping changes taking place in all sectors of public life. Information technologies and the information services market have become the driving force of the modern economy. The present-day developments render that every business function and form of communication is carried out through an ever-twisting environment of information and communication technologies. In the past, only large industrialized countries gained great benefits and profits from doing business with other countries. Nowadays, even developing countries can experience the benefits of such relations. The beforementioned is driven by the globalization of information technologies (Casey, 2011).

In addition to apparent advantages, the evolvement of information and communication technologies creates new problems, as follows: information and technologic inequality between countries, challenges of legal regulation of the Internet, e-commerce and taxation, security and information issues, the risk of psychological effect on human consciousness and society (Kondratenko, 2021).

The state of information inequality in society, in addition to the manipulation of public and individual consciousness, can cause such a negative consequence as the spread of information-related crimes. This primarily concerns the infringement of information ownership.

The promotion of digitalization and the extension of information services facilitate increasing the number of frauds and crimes related to information, information services, information products, and digital technologies.

At the same time, the scope of possible information crimes is very large: from harming a person by theft, destruction, distortion of personal data to social, legal, economic and political problems of society related to cybercrime and corruption at various levels, which lead to breaching fundamentals of the democratic society of a particular country.

2 Risks and threats of digitalization

This fact is confirmed by numerous studies. According to PwC Global Economic Crime and Fraud Survey 2018: Ukrainian findings, domestic and foreign companies face crimes and frauds shown in Figure 1.

By relying on survey results, which indicate a high rate of crime, the author concludes that there is a concern of maintaining a sufficient level of information transparency, which is related to and interdependent on information security.

Improvement of transparency is a basic condition for monitoring and guaranteeing the efficient protection of personal data. Therefore, individuals must be well and adequately informed on a transparent basis about data being collected and processed, for what reasons and terms. They should be aware of their rights if they intend to gain access, modify or delete their data. The main element of transparency should comprise the accessibility of information, which is ensured by the clarity and simplicity of the language used. This is particularly relevant to the online environment and in the context of the development of the information services market (Tykhomyrova, 2011).

In addition to the above threats, from the active introduction of information technology and the advancement of the information services market, other main risks and threats of digitalization include:

– capture of new markets by transnational corporations;
– accumulation of power in the market and strengthening monopolies;
– destabilization of the monetary and credit system;
– growing dependence on companies that are leaders in the field of information and communication technologies.

At the same time, the fear of the dangers of digitalization and the informatization of society has grown significantly.

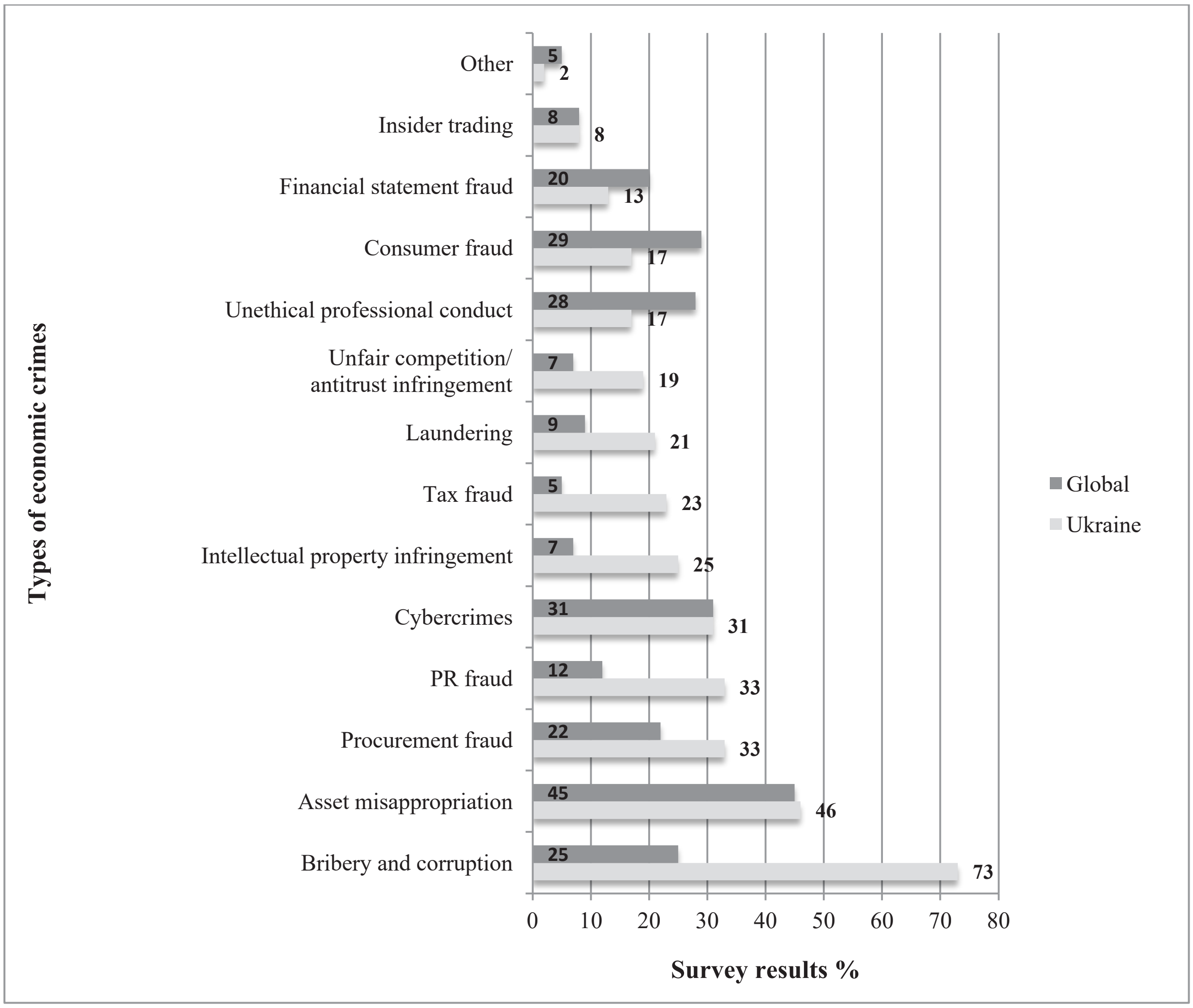

FIGURE 1 Types of economic crimes and frauds which Ukrainian and international companies faced in 2018, % (Rezultaty opytuvannia ukrainskykh orhanizatsiy PwC 2020)

Source: author's development based on the survey results (Rezultaty opytuvannia ukraïnskykh orhanizatsiy PwC 2018)

Most companies are afraid of technological innovation, the emergence of new information products and services, as well as cyber incidents (Pyshchulina, 2019).

Consequently, the study of information security as a factor ensuring the sustainable development of the information services market becoms most relevant.

Technological faked morphosis, filling the existing socio-cultural and political forms with new technologic substance, information and communication networks, carries the danger of creating unpredicted tools for resolving conflicts and crises in society. Unauthorized interference with sensitive information resources of the state, especially of nuclear states, or attempts to manipulate information in the interests of any terrorist group or of one group of countries against other countries can have serious consequences. In such a situation, developed countries are constrained to spend huge financial resources for protecting national electronic resources and information security. Information security usually means the protection of information systems from interference (accidental, intentional), which harms the owners or users of information (Cherevko, 2014).

When it comes to security in general and information security in particular, it is necessary to take into account the target function of the object or actor, as well as security as the ability to implement this function. In this case, the status of the system, which is characterized by the ability of objects and actors to implement their targeted functions, can be defined as a state of security and safety. If the point at issue is active actors, the very concept of "security" is associated with the actor's will to realize own interests.

In other words, the set of living conditions of the actor, one adapted to in the process of work and thus can control, comprises the safety of the actor, the safety of his activities. Moreover, the actor must be able not only to track the dynamics of conditions but also have a real impact on them. From the perspective of information security, it is necessary to consider the information aspect of such impact. Any actor needs to obtain objective information to coordinate his actions.

Information security or infosec is concerned with protecting information from unauthorized access. It is part of information risk management and involves preventing or reducing the probability of unauthorized access, use, disclosure, disruption, deletion, corruption, modification, inspect, or recording.

If a security incident does occur, information security professionals are involved with reducing the negative impact of the incident (Tunggal, 2020). Innovations are rapidly gaining popularity in the market of information services. However, digitalization, the advancement of information technologies, the origin of new information products not only allow expanding communication opportunities but also creating new threats to society and its information security Representatives of the new institutional economic theory believe that the fundamental public good is the specification and protection of property rights (Horniak, Shevchenko, 2013).

In addition to solving the problems of information security of the information services market from the institutional perspective, the general risks of information security in the information services market merit special attention (Figure 2).

In day-to-day operations of each company, many risks can affect the information system due to information security breaches. Social engineering involves the use of psychological techniques to mislead users by providing information or access for attackers. Phishing is one of the most common types of social engineering that is usually conducted using e-mail (Onyshchenko, Petrov, Kobzev, 2017).

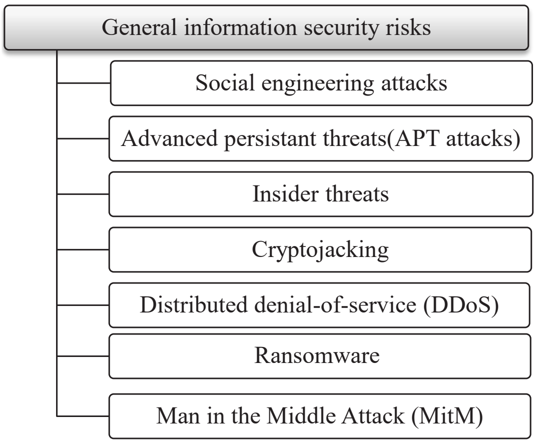
General information security risks
Social engineering attacks
Advanced persistant threats(APT attacks)
Insider threats
Cryptojacking
Distributed denial-of-service (DDoS)
Ransomware
Man in the Middle Attack (MitM)

FIGURE 2 General risks of information security in the information services market

Source: author's development based on (Cassetto, 2019)

During phishing attacks, trespassers pretend to be reliable or legitimate sources that require information or warn users of taking actions. For example, using email, users may be asked to verify personal information or log in to their accounts through an included (malicious) link. If users comply with requirements, attackers may gain access to credentials or other sensitive information.

APTs (advanced persistent threat) are threats in which individuals or groups gain access to your systems and remain for an extended period. Attackers carry out these attacks to collect sensitive information over time or as the groundwork for future attacks. APT attacks are performed by organized groups that may be paid by competing nation-states, terrorist organizations, or industry rivals.

Insider threats are vulnerabilities created by individuals within your organization. These threats may be accidental or intentional, and involve attackers abusing "legitimate" privileges to access systems or information. In the case of accidental threats, employees may unintentionally share or expose information, download malware, or have their credentials stolen (Cassetto, 2019).

Cryptojacking is when attackers abuse your system resources to mine cryptocurrency. Attackers typically accomplish this by tricking users into downloading malware or when users open files with malicious scripts included.

DDoS attacks (distributed denial-of-service attacks) occur when attackers overload servers or resources with requests. Attackers can perform these attacks manually or through botnets, networks of compromised devices used to distribute request sources. The purpose of a DDoS attack is to prevent users from accessing services or to distract teams while other attacks occur.

Ransomware attacks use malware to encrypt your data and hold it for ransom. Typically, attackers demand information, that some action be taken, or payment from an organization in exchange for decrypting data. In these cases, you can only restore data by replacing infected systems with clean backups.

MitM attacks (man-in-the-middle attacks) occur when communications are sent over insecure channels. During these attacks, attackers intercept requests and responses to read the contents, manipulate the data, or redirect users (Cassetto, 2019).

3 Information risk management

In order for the company to cope with external risks in the information services market, it is necessary to build a strong risk management information system. Information risk management is the process of identifying vulnerabilities and threats to information resources used by a company and taking any countermeasures to reduce risks to an acceptable level based on the information value for the company.

The process of risk management is ongoing and iterative in nature, it must be repeated indefinitely as new threats and vulnerabilities emerge, especially external ones. The choice of countermeasures or controls used must strike a balance between productivity, cost, effectiveness, and the information value of the asset being protected.

The likelihood that a threat will use a vulnerability to cause harm creates risk. In the context of information security, the impact is loss of confidentiality, integrity, or availability or all other possible losses (e.g., reputational and financial damages). It is not possible to identify nor mitigate all risks. This remaining risk is called residual risk (Tunggal, 2020).

In addition to considering the general risks of information security in the information services market, to increase the level of information security, every company must adhere to its fundamental principles. The fundamental principles (tenets) of information security are confidentiality, integrity, and availability. Every element of an information security program (and every security control put in place by an entity) should be designed to achieve one or more of these principles. Together, they are called the CIA Triad (Central Intelligence Agency) (Figure 3).

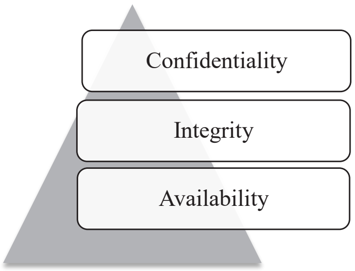

FIGURE 3 Three tenets of information security
Source: author's development based on (Burnette, 2020)

Confidentiality measures are designed to protect against unauthorized disclosure of information. The objective of the confidentiality principle is to ensure that private information remains private and that it can only be viewed or accessed by individuals who need that information in order to complete their job duties.

Integrity involves protection from unauthorized modifications (e.g., add, delete, or change) of data. The principle of integrity is designed to ensure that data can be trusted to be accurate and that it has not been inappropriately modified. Availability is protecting the functionality of support systems and ensuring data is fully available at the point in time (or period requirements) when it is needed by its users. The objective of availability is to ensure that data is available to be used when it is needed to make decisions.

Effective implementation of all three tenets of the security triad is an ideal outcome from an information security perspective. Consider this example: an organization obtains or creates a piece of sensitive data that will be used in the course of its business operations. Because the data is sensitive, that data should only be able to be seen by the people in the organization that need to see it in order to do their jobs. It should be protected from access by unauthorized individuals. This is an example of the principle of confidentiality.

When the individual that needs that piece of data to perform a job duty is ready to utilize it, it must be readily accessible (i.e., online) in a timely and reliable manner so the job task can be completed on time and the company can continue its processing. This describes the principle of availability. And finally, the data will be used in calculations that affect business decisions and investments that will be made by the organization. Therefore, the accuracy of the data is critical to ensure the proper calculations and results upon which decisions will be made. The assurance that the data has not been improperly tampered with and therefore can be trusted when making the calculations and resulting decisions is the principle of integrity (Burnette, 2020).

4 Conclusions

Corporate information security is primarily associated with the improvement of management processes. The interest of each employee in the outcome of the company's operation, the reward that the employee considers adequate and worthy of his efforts, is known to be a very effective method of combating theft within the company. In this context, information theft is nothing new and only differs in the skill level of the participants in the process. It is notorious that in the case of unqualified management of the company, the cost of the information security system may exceed the damage from possible theft (as mentioned above in the case of insufficient IP protection in the information services market).

In addition to compliance with the basic principles of information security by companies that are participants in the information services market, the author proposes implementing the following measures within the company:

– Support of cybersecurity staff of the company. Cybersecurity workers often call the lack of organizational support the biggest concern. The cybersecurity department is often not sufficiently funded to cover current expenses, and the company executives do not pay heed to and do not consider the requests and proposals of the relevant department.
– Annual training for raising awareness of corporate personnel. The two biggest threats experienced by companies are phishing and ransomware attacks, both of which use human errors. If employees who receive phishing emails (which often contain ransomware) cannot detect them, the company is definitely at risk. Employees' misunderstanding of their information protection obligations leads to accidental breaches, abuse of privileges, and data loss.

- Prioritization of company risk assessments. Risk assessment is one of the foreground tasks that an organization must perform when working out its information security program. This is the only way to make sure that the control system chosen by the company meets all the possible risks that the company faces or may face in the future.
- Regular review of company policies and procedures. Policies and procedures are documents that set company rules for data and information processing. The policy provides full details of the company's operation principles, while procedures thoroughly describe how, what and when to do. The evolution of the cyber threat landscape requires companies to review their policies and procedures regularly. If a particular procedure does not work in the company, it should be revised and changed as needed.
- Regular maintenance of corporate appraisal and improvement. Each of these steps refers to the need for regular reviews, but the appraisal and improvement processes are so important that they deserve special attention.
- Introduction of digital signature. A company can expend much time in getting the various signed documents. For example, in companies operating in the services market, the number of transactions that need to be signed immediately may increase directly in the company's office if the CEO is absent from the office. It may weaken sales and customer service. Agreements can be signed with a digital signature online from any point.
- Compliance with international standards that regulate the best practices of information security management in the company.

Therefore, information security in the information services market is a marker of the fundamental difference between the information society and the industrial society. The main hallmark of the information society is its openness. This means a significant reduction and thus the general lack of confidential information for society. The advancement of the information society is not possible without openness. This openness is primarily associated with the decrease of corruption and other economic crimes and fraud, as well as with classified information that must be protected.

References

[1] Rezultaty opytuvannia ukrainskykh orhanizatsiy PwC (2018). Vsesvitnie doslidzhennia ekonomichnykh zlochyniv ta shakhraystva [World Study of Economic Crimes and Fraud]. E-source: https://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf (accessed 27 May 2021).

[2] Rezultaty opytuvannia ukrainskykh orhanizatsiy PwC (2020). Vsesvitnie doslidzhennia ekonomichnykh zlochyniv ta shakhraystva [World Study of Economic Crimes and Fraud]. E-source: https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf (accessed 13 May 2021).

[3] Horniak, O. V., & Shevchenko, M. S. (2013). Prava sobstvennosti v ekonomicheskoj strukture obshchestva: konceptual'nye podhody [Property rights in the economic structure of society: conceptual approaches]. *Economic innovations: Coll. Science. etc. IPREED NAS* (electronic journal), vol. 53, pp. 79–84. E-source: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/71749/08-Gornyak.pdf?sequence=1 (accessed 14 May 2021).

[4] Kondratenko, N. D. (2021). Doslidzhennia informatsiinoi nerivnosti na rynku informatsiinykh posluh [Research of information inequality in the market of information services]. *Technological audit and production reserves*, vol. 57, no. 1, pp. 6–9.

[5] Onyshchenko, Yu. M., Petrov, K. E., & Kobzev, I. V. (2017). Protydiia zlochynam, shcho vchyniaiutsia za dopomohoiu metodiv sotsialnoi inzhenerii v internet [Countering crimes committed with the help of social engineering methods on the Internet]. *Law and security*, vol. 64, no. 1, pp. 63–68.

[6] Pyshchulina, O. (2019). Dvi storony tsyfrovykh tekhnolohii: «tsyfrova dyktatura» abo zberezhennia stiikosti [Two sides of digital technology: "digital dictatorship" or maintaining resilience]. *Razumkov center* (electronic journal). E-source: https://razumkov.org.ua/statti/dvi-storony-tsyfrovykh-tekhnologii-tsyfrova-dyktatura-abo-zberezhennia-stiikosti (accessed 17 May 2021).

[7] Tykhomyrova, Ye. B. (2011). Komunikatyvna polityka YeS: informatsiina bezpeka vs transparentnist [EU communication policy: information security vs transparency]. *Current issues of international relations*, vol. 102, no. 1, pp. 22–28.

[8] Cherevko, O. V. (2014). Teoretychni zasady poniattia informatsiinoi bezpeky ta klasyfikatsiia zahroz systemi informatsiinoho zakhystu [Theoretical foundations of the concept of information security and classification of threats to the information security system]. *Efficient economy* (electronic journal), vol. 5. E-source: http://www.economy.nayka.com.ua/?op=1&z=3304 (accessed 14 May 2021).

[9] Burnette, M. (2020). Three Tenets of Information Security. *The LBMC Family of Companies*. E-source: https://www.lbmc.com/blog/three-tenets-of-information-security/ (accessed 05 May 2021).

[10] Casey, J. (2011). Backgrounder: China's 12th Five-Year Plan, U.S.. *China Economic & Security Review Commission*. E-source: http://www.uscc.gov/researchpapers/2011/12thiveYearPlan_062811.pdf (accessed 14 May 2021).

[11] Cassetto, O. (2019). Information security (InfoSec): The Complete Guide. *Exabeam*. E-source: https://www.exabeam.com/information-security/information-security/ (accessed 20 May 2021).

[12] Tunggal, A. T. (2020). What is Information Security? *UpGuard*. E-source: https://www.upguard.com/blog/information-security (accessed 18 May 2021).