Risks and Vulnerabilities in Online Commerce

Alin-Flavius MARTA[1]
Margareta Stela FLORESCU[2]
Laurentiu COROBAN[3]

Abstract

In today's society, knowledge of the use of the Internet and communication networks has become a necessity. Competences in the use of technology, both in daily activities and in professional activity, are indispensable for modern man.

Society evolves at a dizzying pace, people's lack of time and the opportunities generated by the possibility of everything being accessed from the comfort of home is a trend that seems to be unstoppable. Making transactions online offers advantages that any other market is hard to compete with, from your home or office chair, you can compare multiple product offers, prices, etc. and choose the one that suits your needs, without wasting time physically going to the store, and for comparison by visiting several stores. All these aspects weighed enormously and encouraged online trade, the market where demand and supply are a click away, having an unprecedented growth in the recent history of mankind, the upward evolution of the number of transactions in the online environment being inevitable.

Considering the trend of online commerce, the role of the study is to identify the risks and vulnerabilities manifested in these transactions, the Internet being exposed to cyber criminality, and beyond them, what would be the way in which these vulnerabilities and risks could be treated and countered.

Keywords: *E-commerce, risks electronics, crime cybernetics, security cybernetics, e-banking risks*

JEL classification: L81, E32, G29
DOI: 10.24818/RMCI.2023.2.210

Introduction

In the conditions of economic development and digitization, crime in the form of shoplifting has decreased significantly. The same cannot be said for cybercrime, with the move of commerce online providing the opportunity for another type of crime. In recent years, mainly after the start of the Covid-19 pandemic, e-commerce has become a favorite target of those who deal with crimes, being one of the sectors that has suffered the most attacks from cybercriminals. This trend is mainly due to the increase in demand for products and services through online

[1] Marta Alin-Flavius, West University of Timisoara, Romania: alin.marta79@e-uvt.ro
[2] Florescu Margareta Stela, Bucharest University of Economic Studies, Romania, margareta.florescu@ari.ase.ro
[3] Coroban Laurentiu, West University of Timisoara, Romania, dorucoroban@yahoo.com

market platforms, websites, etc. e-commerce exploding, as it were, as a result of the pandemic.

With the rise of online sales have come more opportunities for those prone to online crime. Any operation performed through e-commerce requires personal data, card information, various platform security measures, etc., so there were and are sensitive points that allowed hackers to easily exploit these so-called security gaps.

E-commerce significantly simplifies the life of the individual by accessing various markets, from various corners of the world, in real time.

The use of online transactions in trade operations is one of the causes that have determined the need for transparency in the evolution of the economic market. Unlike the situation around two decades ago, there has been a major increase in the transparency of the economic market.

The interaction between economic operators was facilitated by means of communication such as the telegraph and the telephone. Once technology evolved and the Internet appeared, the communication between suppliers and consumers and the transparency of the economic market experienced an unprecedented momentum until that time.

"Online commercial transactions offer real advantages in terms of the desired product, its quality, price, identification of certain offers or discounts, comparison with similar products from other suppliers, access to international markets, all from the comfort of your own home."(European Commission, EU study on the legal analysis...2009).

Online trade, risks and vulnerabilities

As far as the consumer is concerned, the benefits are visible. To the same extent, e-commerce also creates opportunities for suppliers, such as reducing expenses and, as a consequence, increasing profits, increasing the number of customers, access to the global market, sharing information and technology, the possibility of developing departments with activity in the innovation and research sectors, in order to improve commercial processes based on the facilities of the Internet.

The collaboration between the factors involved in e-commerce operations, both between the different departments within the company, and between the company and other companies with which it collaborates, in order to fulfill its mission - the provision of goods and services, is simplified by the transparency that the use of technology an imprint of the economic market.

E-commerce has the advantage of removing any restriction in communication because through the use of technology it is possible to connect between the actors involved at any time and from any place, in real time. Thus, the exchange of information is carried out quickly, which is an advantage for both suppliers and customers.

On the other hand, technology provides access to information about markets, customers, suppliers, resources, facilitating analysis and studies in order to improve the company's performance.

At the same time, online sales offer the advantage of making purchases at the best price, being accessible in real time all the information regarding the price charged by several suppliers regardless of whether it is for the same product or for similar services. Thus, the buyer can initially analyze and compare the price, but later also the delivery conditions, the warranty offered, etc. we say: " can purchase a product or service at the best price in relation to the quality and characteristics sought".

Also, online commerce offers the advantage of saving time by the fact that, first of all, purchases no longer involve physical travel to certain points of sale, work points of suppliers who have a set schedule and which limit us as visiting hours, and secondly, several goods or services can be purchased at the same time, at the most advantageous (competitive) prices.

Adapting stocks by tracking information about them leads to an increase in the efficiency of suppliers of goods and services. Product demand analyzes facilitate supply adjustment, stock replenishment, with direct consequences in reducing expenses and immediate profit growth.

E-commerce requires a small number of employees, which means a reduction in personnel expenses. At the same time, financial resources can be redirected from personnel costs to other sectors, such as improving the quality of products and services offered, investing in technology and/or software, improving existing human resources, etc.

Taking into account the fact that the Internet offers unlimited access to a global market, regardless of the size of the company, efforts are needed for investments in human resource training to keep up with the trend of changes generated by the diversity of economic operators in the market, where the characteristics, culture and way of working specific to each of them allows to stimulate creativity and increase employee involvement in promoting the company, respectively improving the way it responds to market requirements and challenges.

The image that the company has in the market directly depends on the training and the way of involvement of the human resources available to the company.

In a globalized market, the company's headquarters or workplaces have little importance compared to the image it has in front of customers or collaborators. This aspect is a great advantage for developing companies. Only in this way, electronic commerce determines an increase in the transparency of the economic market and productivity. *"Technology offers opportunities to both customers and suppliers, purchases take place quickly. We can consider electronic commerce as the perfect competitive model."*(European Commission, EU study on the legal analysis... 2009).

However, there are certain vulnerabilities of the use of the Internet in the commercial operations of trade for goods and services, due to the lack of trust in data

security, technical deficiencies, insufficient or unsuited logistical resources, as well as the lack of information of the population.

As a result, e-commerce still needs time to gain the trust of economic operators, and they, in turn, to find the resources to exploit its full potential.

In this context, we can see sustained efforts in society to promote information on this form of commerce, to amend the legislation on electronic commerce and to implement more and more effective data security standards.

A. IT risks in electronic commerce

When we talk about the risk generated by access to electronic platforms, we must refer to all the problems identified as possible to arise in the operations specific to electronic commerce. The Internet was created to facilitate the exchange of data and information, but conducting business online was not its purpose in itself.

Over time, e-commerce has evolved, prompting an anticipated development of both the methods of identifying and mitigating electronic risks and the methods of cybercriminals.

"Among the major electronic risks we list the spread of viruses that generate errors and/or compromise the system, as well as the activity carried out by hackers in the online environment."(Graham , J., Howard, R. &Olson, R., 2011, New York, p. 41).

Regarding hackers, their methods are advanced, they seem to be in symbiosis with technological evolution, representing a real danger for all those who operate in this e-commerce market, whether companies or customers. The collection of the data of the latter, but also of the companies, by accessing (breaking) the databases with the information related to the cards, or intervening on these databases, by deleting or modifying them, represents the major risk of electronic commerce.

B. E-commerce and cybercrime

The main vulnerability of e-commerce , therefore, is cybercrime. The fight against this form of crime is a constant concern, both from the perspective of companies and from the perspective of customers.

From the perspective of companies, cybercrimes represent a real and direct danger, when the passive subject of the crime is the company itself, its patrimony being affected (for example, by stealing sums of money from the company's accounts and/or blocking the company's web page), but it can also represent an indirect danger when the victims are customers of the company, who have trusted and provided sensitive data. In the latter situation, the company's reputation and confidence in its capabilities to ensure data security are seriously affected, and the result will result in a reduction in the number of customers and, by way of consequence, a reduction in the profit made or reported by the company.

Implementing effective security standards is essential for all businesses that conduct e-commerce.

Among the forms of cybercrime we find phishing, computer viruses, denial of service attacks. In recent years, combating cybercrime has become a general concern of governments, a challenge for states and for the creation of a legal framework to limit the interventions of those with criminal intentions, providing the safety of electronic commerce, that conducive environment for future economic development.

To counter cybercrime, we need to know what the main types of cyberattacks are:

1. Computer virus:*"is a malicious program, which spreads between computers, installs itself and affects the software system or files in the computer."*(Lotz, V., Kaluvuri, S., Di Cerbo, F. &Sabetta, A., 2012, NTMS, p. 3);
2. Phishing attacks: the victim accesses an e-mail message that leads to a fictitious website where confidential data is requested;
3. Botnet: involves a hacker taking control of the compromised computer;
4. Spoofing: involves exploiting a person's identity to convince another person to divulge personal data, which will then be used for unauthorized purposes;
5. E-bank theft: involves accessing the banking system and transferring funds to an account that can only be accessed by the hacker;
6. Netspionage: involves accessing a person's computer or their online account by a hacker in order to obtain confidential information;
7. Online credit card fraud: it involves illegal access to the data of a bank card, with the aim of carrying out unauthorized transactions;
8. Online denial of service: involves the use of viruses or other techniques to make a network or computer inaccessible;
9. *"Software piracy: represents an act of stealing a software, including by copying, distributing, modifying or selling it;*
10. *Spam: refers to unsolicited emails."*(Rao, J., & Reiley, D., 2012, Journal of Economic Perspectives, p. 89).

Cybercrime is the main reason many people avoid doing business online. Electronic commerce requires the identification of risks and their consequences.

Next, we will address the topic of web insurance services.

"This type of service provides data about the credibility of websites. There are 4 services of this type: BBBOnline, Trust Services, TRUSTe and VeriSign.

The use of one of these services, visible through the application of the specific seal, offers guarantees regarding certain aspects of the company's activity." (Coskun, V., Ok, K. & Ozdenizci, B., 2012, New York, p. 56).

C. Internet Security Certification Services

C.1 *VeriSign* – provides digital certificates regarding the authenticity of the site and the protection of communicated data (forms, financial data) against unauthorized collection or modification.

C.2 *TRUSTe – "using the services provided by this company implies that the website visitor will be notified of the personal data that will be collected, the options regarding data collection; how the collected data will be used; who collects the data and how it will be shared data, data security procedures, etc.."*(Graham, J., Howard, R. & Olson, R., 2011, New York, p. 71).

C.3 *Trust Services* - includes WebTrust and SysTrust and is *"a set of practices based on common principles and criteria, the purpose of which is to provide guidance or advice regarding information technology systems. The American Institute of Certified Public Accountants and the Institute The Canadian Association of Certified Public Accountants has developed a set of standards that address, among other things, the confidentiality of operations, the security of personal data and the system accessing the site, and the integrity of transactions."* (Lotz, V., Kaluvuri, S., Di Cerbo, F. & Sabetta, A., 2012, NTMS, p. 3).

C.4 *BBBOnLine* – a company whose website has the BBBOnLine seal is part of the local Better Business Bureau, has been on the market for at least 1 year, complies with the BBB's standards of truth in advertising and has undertaken to cooperate with the BBB in order to resolve consumer disputes, regarding the goods or services sold on its website.

D. The concept of e-Security

The notion of "e-security", also known as cyber security or IT, generally refers to the set of measures, procedures and technological solutions used to secure systems and networks against cyber attacks. *"Between this branch of computer security and the Internet network there is a close connection, taking into account the need to ensure the security of the browser and the network, as well as to identify, reduce and eliminate the risks and vulnerabilities specific to the use of the Internet network for the exchange of information."*(Graham, J., Howard, R. & Olson, R., 2011, New York, p. 74).

Exchanging information over the Internet poses a high risk of digital phishing attacks. In order to eliminate this vulnerability, a series of specific measures have been implemented, among which one of the most used measures is the encryption of the transmitted data.

In addition to the obvious and indisputable advantages of using the Internet, there are also a number of disadvantages generated by the essential need to protect all processed data, a task that has become increasingly difficult to fulfill. Although the technological field knows a permanent and constant evolution, the methods and means of committing cyber attacks evolve at the same pace as the development of technology, being a challenge for combating " criminal " acts . In other words, the

evolution of technology supports the development of the means necessary to protect data and information, but it represents, at the same time, a source for new forms of cyber attacks.

In this context, ensuring the security of systems and networks has opened the doors to an independent field that, remarkably, offers opportunities for investment and innovation.

E-security aims to *"ensure security in the field of electronic commerce, by implementing the necessary measures to protect computers and managed data."*(Coskun, V., Ok, K. & Ozdenizci, B., 2012, New York, p. 91).

The field of cyber security is a complex, vast one that requires in-depth specialized knowledge or continuous improvement. The protection of managed data refers to the implementation of appropriate measures to prevent the unauthorized transfer, modification and/or deletion, or compromising, in any form, of information and managed data.

Thus, *e-security* aims to ensure the security of information, the computer and the Internet network used by customers, suppliers, etc. for data communication.

E. Data security management in e-commerce:

Economic and technological development and the globalization of resources, markets and finance, represent a series of factors that have determined the move of connections from the business environment to the online space. Today, most discussions, negotiations, interactions specific to the business environment take place within platforms, applications that use the Internet. The indisputable advantage is the possibility of real-time and useful connection between factors located in different geographical areas of the world.

But, in the context of these discussions, which often contain sensitive data, the issue of securing data and communication channels arises again. The use of accounts and passwords for authentication, authorization of operations, encryption and ensuring data integrity, becomes imperative.

Electronic security is a priority for both corporations and governments, as it is known that a data security incident can have devastating consequences for the service provider and their recipient.

E-security ensures*"the implementation of mechanisms to protect data and online services provided and identifies risks and vulnerabilities in order to prevent any cyber attack."*(Berthome, P., Fecherolle, T. & Others, 2012, ARES, p. 389).

F. Vulnerabilities and risks cyber in e-commerce

The development of electronic commerce essentially depends on ensuring the security of transactions , and here it is necessary to identify the existing vulnerabilities and risks:

F.1 Unauthorized access to information is considered the main risk. It is the result of ineffective data and network protection measures, giving the possibility

of easy access by unauthorized persons to the confidential information of companies. Unauthorized access to this data, by hackers, damages both materially, but also has an effect on the image of the company. The situation is much more complicated when data obtained illegally can be used to commit crimes.

F.2 Loss of customer trust - as we have already presented, a cyber attack on a company, the result of which is the compromise of data and information, seriously damages its image.

F.3 Interruption of the services provided – refers to situations in which the services offered by the company cannot be provided because, following a denial of service attack, the site no longer functions or functions with limitations.

F.4 Lack of crisis procedures – the danger of cyber attacks increases with the development of e-commerce. It is necessary and very important that at the level of companies there is a procedure applicable immediately in crisis situations, with measures to counter attacks.

G. The need to implement the E-Security concept:

The implementation of measures to prevent cyber attacks in any situation and guaranteed is impossible. Therefore, network security measures involve, on the one hand, the implementation of protocols to prevent attacks or intrusions and, on the other hand, their identification once they have occurred.

Network security refers to the totality of systems implemented to protect the network and data, regardless of whether it is a LAN (local area - computers connected over a small distance) or WAN (worldwide - the Internet).

"One of the devices used to ensure network security are firewalls, which monitor and filter data traffic using certain security keys. In some companies, firewalls are also used to encrypt data traffic between internal networks so that prevent unauthorized access to certain data."(Coskun, V., Ok, K. & Ozdenizci, B., 2012, New York, p. 104).

The second solution is "intrusion detection – ensuring network and data security by monitoring and filtering data traffic, identifying any activity that is suspicious or that violates company rules and/or policies, and blocking the activity as appropriate."(Lotz, V., Kaluvuri, S., Di Cerbo, F. & Sabetta, A., 2012, NTMS, p. 5).

Firewalls vary and can be software or hardware, multifunctional, or designed to identify certain clearly defined characteristics. *For example:* A network sniffer is a device used to examine data traffic on a network segment. Over time, this device has been adopted by hackers for unauthorized access to certain data.

H. Security tools_electronics:

Among the tools implemented to ensure the security of operations and transactions in electronic commerce, we find:

H.1 Hardware and software firewalls;

H.2 Digital signatures – prove the authenticity of trafficked data;
H.3 Digital certificates – allow the use of digital signatures as a means of proving the authenticity of data;
H.4 Passwords – ensure the authenticity of digital information and prevent unauthorized access to it;
H.5 Public key infrastructure – data exchange involves the use of cryptographic key pairs;
H.6 Encryption software – ensures the security of trafficked information by the fact that it can only be decrypted by a person who holds the decryption key;
H.7 Retinal, fingerprint and/or voice scanning biometric systems, etc.;
H.8 Blockers.

I. Security in the field of electronic commerce

The security of e-commerce must be analyzed in the context where a large part of the companies' activity involves *"trafficking data through Internet networks, data security has become a priority."*(Rao, J., & Reiley, D., 2012, Journal of Economic Perspectives, p. 89).

E-Commerce Security refers to a set of globally established rules and procedures to ensure the security of online transactions and identify the main threats to e-commerce operations.

Thus we consider three aspects :

i) Securing data and documents transferred via the Internet;
ii) Securing transactions;
iii) Securing the network used in online commerce.

The basics of computer security:

Ensuring computer security covers the following principles and notions:

✓ Confidentiality of data and information – implies the implementation of the necessary measures in order to prevent the access of unauthorized persons and/or the interception of transmitted information.

✓ Data integrity – presupposes the implementation of the necessary measures so that the transmitted information is not altered by modification, deletion and/or other means;

✓ Data availability – the transmitted data must be accessible at any time, by authorized persons;

✓ Authenticity – presupposes the implementation of an authentication system through which only the authorized person can access trafficked data and information,

✓ Implementation of a system that does not allow rejection of the order, payment or message;

✓ Encrypting information – so that it can only be accessed by the person who holds the decryption key,

- ✓ The information must be accessible to the integrity audit;
- ✓ Fraud committed by providing incorrect or incomplete data.

J. Security management of computer trading Systems

Among other things, *"any company's security policy must respond to essential requirements and objectives."* (Kaluvuri, S., Koshutanski, H., Di Cerbo, F. & Maña, A., 2013, ICWS, p. 540):

- ❖ Identification of risks and vulnerabilities;
- ❖ Identification of confidential data and information;
- ❖ Regulation of methods and means of ensuring data confidentiality;
- ❖ Identifying the most suitable authentication system;
- ❖ Identifying and implementing an effective system for detecting and removing unauthorized access to the network;
- ❖ Establishing the person responsible for the e-business infrastructure;
- ❖ Establishing a plan of measures applicable in crisis or emergency situations, so as to ensure the continuity of service provision.
- ❖ The main features of an effective and sustainable security policy:
- ❖ Clear establishment of purpose and objectives;
- ❖ Compliance related compensation;
- ❖ Existence of mechanisms to allow enforcement and verification of compliance;
- ❖ Implementation of a system based on access - authentication - authorization;
- ❖ Establishing a data back-up procedure;
- ❖ Establishing a work procedure and data recovery in the event of destruction caused by force majeure.

The main security measures that can be implemented:

- Data encryption – data is transmitted in a message that can only be accessed by a person who has the decryption key;
- Digital signature – ensures the authenticity of trafficked data;
- *"The security certificate – allows the verification of the identity of the person or the site."*(Lotz, V., Kaluvuri, S., Di Cerbo, F. &Sabetta, A., 2012, NTMS, p. 4).

The e-security design project is a process that includes 6 stages:

1) Identification of risks, awareness of them at company level and development of risk management. Implementing effective security policies depends on understanding the importance of information and its security across the organization. *"Regardless of the hierarchical level at which they are located, each individual within the company must be aware of their own responsibility in terms of securing the data they manage".*(Berthome, P., Fecherolle , T. & Others, 2012, ARES, p. 391).

2) Risk analysis and assessment - is a process of identifying risks, threats, vulnerabilities and possible expenses generated. In this process, the risk is established as the ratio between threats, vulnerabilities and the costs generated by them, on the one hand, and the cost of resources used to implement measures to identify them and remove them, on the other hand.

3) Establishing an e-commerce security policy in correlation with systematic risk management.

An organization's security policy is one of the pillars on which its image and prestige are built and, as a consequence, the trust that customers place in it. It must address internal and external factors, human, financial and material resources, management and execution function accountability, risks and vulnerabilities at all levels.

The privacy policy must address six goals of e-commerce security: confidentiality , integrity, availability, legitimate use, auditing, and non-repudiation.

4) Establishing clear, concise and efficient procedures aimed at securing the e-business infrastructure. This stage is a technological one . It must target every component of the infrastructure (eg cryptography and digital signature technology). Work procedures must ensure the greatest economic efficiency and be proportionate to the identified possible risks and vulnerabilities.

5) Establishing the residual risk. In the risk analysis and assessment process, those risks will be identified which, once the work procedures are implemented, remain uncovered. In order to manage these risks, an insurance mechanism must be implemented, remaining under evaluation from the perspective of probability and financial consequences.

6) Monitoring the implementation and constant adaptation of the system. Permanent changes in the technology sector, the emergence of new risks and vulnerabilities, give the process of implementing e-business security a dynamic character. As a result, it is important that it is permanently adapted to new technological realities, which requires an effective monitoring system and the regulation of a feedback mechanism.

Risk assessment

Securing the data and the network used by the company in carrying out its specific activity requires a constant process of analysis and assessment of risks and vulnerabilities, monitoring trafficked data and network activity, followed by the adaptation, according to needs, of work procedures and security systems. information protection. The magnitude of the risks must be evaluated by referring to the possible negative consequences that they can produce for the company and the costs generated by the countermeasures.

The purpose of this risk assessment process is to identify the most effective risk management and data protection measures.

Depending on the specifics of the company's operations and transactions on the Internet, risk management measures are more complex or simpler.

Among these we mention:

- Installation of antivirus programs or firewall devices;
- Constant software update;
- Establishing highly secure passwords;
- Paying extra attention to incoming email messages, especially if the sender is unknown.

Where e-commerce operations are more sensitive, more complex data security measures are required, such as a data security policy and the development of crisis response plans and even outsourcing of security services.

Along with the implementation of a sophisticated security policy, the authentication possibilities of the company's collaborators must be taken into account, so that online operations and transactions continue to take place safely.

One of the most common types of technology is card and pin authentication. Authentication is based on a password, a token or even a fingerprint.

Authentication is only one step in the data and information security procedure. It is part of the regulated data security policy.

The main risks identified in e-commerce are viruses, but the activity of hackers and the copying of credit card data by them are classified as business, technological and informational risks.

Risk classification:

I. *"Risks that refer to the information and data existing on the site and that are specific to e-commerce operations."*(Kaluvuri, S., Koshutanski, H., Di Cerbo, F. & Maña, A., 2013, ICWS, p. 542).

Examples:

- The information published on the company's website may expose it to slanderous attacks on it, with serious consequences on its image;
- Possible infringements of intellectual property rights as a result of the information posted, the digital transformation processes and, as the case may be, the brands used by the site's creators, as well as the disputes that may arise in these situations;
- Possible trade secret violations;
- *"Disclosure of personal data;*
- *Posting information or data with biased content;*
- *Violation of regulations specific to certain states;*
- *Disclosure of Card Data Used in Online Transactions."*(Graham, J., Howard, R. & Olson, R., 2011, New York, p. 133).

II. Technological risks refer to *"risks associated with hardware, software, data transmission security and database security. They are a result of the incorrect use of technology."*(Lotz, V., Kaluvuri, S., Di Cerbo, F. &Sabetta , A., 2012, NTMS, p. 5).

Examples:

- The development of the software component contains errors that may allow unauthorized access to data or infringement of copyrights;
- Unauthorized access to the company website;
- Installation of computer viruses;
- Blocking the server that provides access to the Internet network;
- The hardware component is not adapted to the current technological context;
- Internet services provided by the operator have a poor performance with constant interruptions;
- Difficulties encountered in trying to contact Internet providers;
- Risks generated by the technological capabilities of processing products and data.

III. Business risks refer to those risks that concern the collaboration with customers, but also the products and services provided. At the same time, this category of risks addresses the managerial perspective of the business and interactions at the level of employees.

Examples:

- "The information presented on the site generates image damage for the company;
- Posting data that may harm the image of third parties, employees or customers and that attract the company's responsibility;
- The presentation of data or information, globally, that contravenes the legal regulations of certain states;
- Illegal holding of contests on the company's website;
- Poor site maintenance;
- Recruitment of employees by competing companies;
- Poor communication with suppliers and customers, ineffective marketing strategies, which are often due to poor professional training of the responsible staff;
- The lack of products in stock and the impossibility of fulfilling orders;
- Exaggerated transport expenses, all due to ineffective communication between company collaborators and employees, or at the level of decision-makers;
- Establishing ineffective return policies;
- The company's activity is excessively dependent on the Internet provider;
- The risks generated by the lack of security regarding purchased domains and extensions."(Clark, R.M., Hakim, S., 2014, New York, p. 28).

Giving a reduced importance to the risks presented may have patrimonial consequences generated by:

✓ *"Disclosure or compromise of data, fraud or the impossibility of providing services."*(Berthome, P., Fecherolle, T. & Others, 2012, ARES, p. 395);

✓ Fines or compensations generated by the impossibility of providing services, late provision of goods and services, violation of legal provisions in the field of personal or confidential data.

E-commerce threats broadly refer to the real opportunity to intentionally disrupt business. "These can be internal, when they come from the participation of company employees, but they can also be external.

- *Threats aimed at intellectual property rights, for example : use of the domain name without the owner's consent, software piracy, etc.;*
- *Threats involving computer virus infection, the most common example being the Trojan horse;*
- *Threats related to the operation of communication channels, and here as an example is the use of sniffer devices;*
- *Threats related to the operation of servers - for example spam."*(Clark, R.M., Hakim, S., 2014, New York, p. 44).

In order to reduce security threats, some steps must be followed:

a) Analysis and assessment of threats, of the possible costs generated by the occurrence of the risks and the costs generated by the measures to remove the threat;
b) The development and implementation of the security policy aimed at:
   - ✓ Protected information and property;
   - ✓ Identified vulnerabilities;
   - ✓ Threats and risks to be addressed,
   - ✓ Personnel with responsibilities in its implementation;
   - ✓ Rules of conduct.
c) Establishing a plan regarding the implementation of the security policy and monitoring compliance with the implementation stages and deadlines;
d) Establishing the personnel or structure responsible for implementing and monitoring compliance with the security policy;
e) Checking the implementation of the policy, simultaneously with the fulfillment of the objectives, with the analysis of the difficulties encountered, respectively the application of revision and adaptation measures.

K. The difficulties of nature legal:

The conduct of commercial operations in the online space, as a phenomenon characteristic of the last decades, still arouses mistrust in terms of their legal regulation among many economic operators in the market or even among customers.

Since initially the way in which the judicial bodies, entitled to apply the legal provisions, in the case of these economic transactions, was not very clear, in the early stages of the development of electronic commerce there were reluctance to carry out online commerce operations.

To encourage operations and transactions in this space, of online platforms, state governments have developed a technologically neutral legal framework. This legal framework has been implemented or is being implemented in most states.

However, there are still difficulties and deficiencies identified in practice, which are subject to regulation as the various disputes are resolved by judicial bodies.

The concept of e-banking from the perspective of cyber risks

E-banking applications have beyond indisputable advantages, at least in terms of online transactions, a series of specific security risks, which can be classified as follows:

- Serious risks, when it refers to a serious, intentional breach of legal regulations aimed at data security (for example fraud), most often attracting the criminal liability of the culprits;
- Risks generated by occasional attacks by hackers and which usually cause temporary blocking of the site;
- Risks generated by the poor development of software and hardware systems, which can generate various security incidents.

In order to improve the security system, we consider the following aspects important:

Developing and implementing the most effective systems and network security control procedures.

Monitoring and double-checking the effectiveness of security controls, and constantly reviewing procedures.

Continuous professional training of personnel involved in the implementation, monitoring and assurance of cyber security.

The security of transactions on the Internet is ensured by the use of certain protocols:

1. *Secure SocketsLayer (SSL)* is also the most common. It ensures secure communication, using the following parameters: authentication - encryption - integrity - non-repeatability.
2. *The SET protocol* is the one that defines the secure electronic transaction, being developed by MasterCard and Visa, with use for the active security of electronic payments.

Components:

- The software component for the holder 's digital wallet card , purchases being realized through point *and click* interface.

- ❖ The software component for economic operators is the one that ensures the security of communication between economic operators, clients and banks, too a closed circuit;
- ❖ The Server Gateway software component that provides the payment automatic;
- ❖ The software component for the certification authority, with use at the level institutions banking, for issuing digital certificates .

Firewall:

Firewall systems monitor and control data traffic and network activity, isolating a private network from the public network in order to identify suspicious activity and prevent external attacks on the site by protecting the internal network.

Firewalls generally fall into two categories: gateway applications and proxy servers.

Firewalls are defined as a system positioned between two networks that filters data traffic both in and out of the private network and prevents unauthorized data traffic from entering the network. A firewall protects the network from cyber virus attacks, enforces the development of a data access control policy and allows the removal of network intrusions (hackers, viruses, etc.). Filtering of the data that is trafficked in the network is carried out based on rules regarding the recipient's and/or sender's address, the protocol used, etc.

The firewall device can be used to protect the applications running on the system and the services. A firewall device is composed of one or more host devices and routers, as well as a number of sophisticated security measures.

L. Viruses cyber and e-commerce sites

A computer virus is a small program that is installed without the consent of the user of a computer system, that spreads from one computer system to another and that can cause damage to the software and hardware components of a computer. This type of malware is developed with the intention of gaining unauthorized access to a computer without the user's knowledge, in order to permanently or temporarily block the use of the computer or certain programs or components.

Certain categories of viruses do not cause damage to the infected system, their activity consists only of constant replication, unlike other categories that seriously affect the performance of the computer. It can compromise or modify data, files, documents and access information about computer activity. By analyzing how these malware programs work, we can identify the types of reactions that occur in the infected host system.

Regardless of the type of virus, it is not harmless and should be removed.

Viruses are spread through files sent via e-mail messages, through the use of CDs, external memories, etc. The virus is activated when the infected document is accessed.

"Deficiencies in the design of software systems or the use of network file sharing programs without a minimum of security measures are among the

main causes of computer virus infection. "(Clark, R.M., Hakim, S., 2014, New York, p. 67).

Computer virus infection can be determined by analyzing:

- Possible changes in the computer's operating mode;
- Deficiencies and errors in the operation of the computer and running programs;
- Alerts generated by the software system about the existence of an installed virus, except where this software component is the target of the virus or if it does not work;
- The appearance of certain messages that mock the user;
- Sending messages without the user's intention;
- Compromise or delete certain files without the user's consent.

The identification of an infection with a computer virus depends on the ability of the antivirus program installed on the user's computer, but also on the latter's skills to notice possible indications that may lead to the conclusion that a virus has been installed on the computer. In the situation where the activity of the virus consists in deleting some documents or sending some messages, things are visible. In the situation where the attack is more sophisticated and it becomes more complicated for the user to identify the existence of the installed virus.

Conclusions

We live in a digital age, where daily life depends on information and technology, and in this evolution the Internet plays a particularly important role.

We live in a consumption-based society where e-commerce and traditional commerce are interconnected.

The methods of trade have not changed, what has changed is only the environment in which trade takes place, from physical to online, the change being favored by innovation in technology, access to information, openness to international markets, easy communication over time real, and not long since the Covid-19 pandemic.

At the same time, this change generates new opportunities for increasing the profits and performances of the companies, determines a real and significant increase in the transparency of the market, with advantages for the companies, but also for the customers, being beneficial to the functioning mechanisms of the market.

This type of trade is, moreover, the most concrete form of the free market, where the risks and vulnerabilities of the systems must be assessed and eliminated, even if this often involves some costs.

On the other hand, all Internet users must be fully aware of the need to acquire the components of cyber security culture and try, as far as possible for everyone, to implement the latest and most effective means of computer security to ensure a safe electronic commerce.

References

1. European Commission, (2009). EU study on the legal analysis of a single market for the information society: New rules for a new age?
2. Graham, J., Howard, R. & Olson, R., (2011). Cyber security essentials, CRC press, New York, p. 41, 71, 74, 133.
3. Lotz, V., Kaluvuri, S., Di Cerbo, F. & Sabetta, A., (2012). Towards security certification schemes for the internet of services. In: 5th International Conference on New Technologies, Mobility and Security (NTMS), p. 3, 4, 5.
4. Rao, J., &Reiley, D., (2012). The economics of spam. Journal of Economic Perspectives, 26(3), p. 89.
5. Coskun, V., Ok, K. &Ozdenizci, B., (2012). Near Field Communication (NFC): From Theory to Practice. Wiley, New York, p. 56, 91, 104.
6. Berthome, P., Fecherolle, T. & Others, (2012). Repackaging android applications for auditing access to private data. In: Proceedings of the 7th International Conference on Availability, Reliability and Security (ARES), p. 389, 391, 395.
7. Kaluvuri, S., Koshutanski, H., Di Cerbo, F. & Maña, A., (2013). Security assurance of services through digital security certificates. In: 2013 IEEE 20th International Conference on Web Services (ICWS), p. 540, 542.
8. Clark, R.M., Hakim, S., (2014). Cyber-Physical Security - Springer Nature, New York, p. 28, 44, 67.