OPERATIONAL RISK & CYBERSECURITY

Carmen Răduţ[1],
Laura Pănoiu[2]

Abstract

The impact of the Internet has had strong growth in the last two decades. The entire economy depends on ICT. The open and free cybernetic space, promoted social and political inclusion allowing easily interaction and exchange of information between communities and citizens from different countries. The Information and communication technology has become the backbone of our economy determining economic growth. Complex systems in key sectors of the economy such as finance, healthcare, energy and transport use powerful computer systems. Meanwhile many business models are built on the continuous availability of the Internet and the proper functioning of the informatics systems. The online environment requires high reliability, protection incidents, malicious activity or abuse. Cyber criminals are using increasingly sophisticated methods to steal critical data or economic espionage activities in cyber space. All these factors explain why governments worldwide have begun to develop strategies and act properly in cyberspace as an important international issue. The paper has a special goal, to approach informatical security segments concerning operational risks generated by the informatic systems used by regulated entities authorized / approved and / or supervised by the FSA.

Key Words: cybersecurity, operational risk

JEL Classification: L86, L96, M15

1. Introduction

For the cybernetic space to remain open and free, the same norms, principles and values that the European Union supports offline should also be supported online. The fundamental rights, democracy and the rule of law require protection in the cybernetic space. Our freedom and prosperity rely more and more on an innovative and robust internet, and it will continue to develop if the private sector and the civil society will sustain its growth. Online freedom means both safety and security. The cybernetic space should be protected from incidents, malicious activities and abusive use. In the past years it was found that the digital environment brings forth enormous benefits, but it is also vulnerable. The number of cybernetic security incidents, either intentional or by mistake, is rising at an alarming pace and this might disturb essential services which we take for granted, such as the supply of drinking water, electricity, healthcare or mobile phone services. EU's economy is already affected by cybernetic criminal acts targeted towards the private sector and individuals. Cybernetic criminals use methods that are more sophisticated in order to gain access to information systems, stealing critical data or asking for ransoms. The development in the cybernetic space of economic espionage and ordered state services represent a new category of threats towards national administrations and companies in EU.

Information regarding the cybernetic security now:

1. There are approximately 150.000 computer viruses in circulation every day and 148.000 computers compromised every day.

2. According to the World Economic Forum, there is a probability of 10% that in the next ten years there will be damage done to the critical information infrastructures, which could lead to 250 billion dollars in damages.

3. Cybernetic criminality is guilty of the biggest part of incidents regarding information security. Symantec estimates that the victims of cybernetic criminality worldwide lose 290

[1]Conf.univ.dr., Universitatea Constantin Brâncoveanu Piteşti, F.M.M.A.E. Rm. Vâlcea, c_radut@yahoo.com
[2]Conf.univ.dr., Universitatea Constantin Brâncoveanu Piteşti, F.M.M.A.E. Rm. Vâlcea

billion EUR each year, while a McAfee study shows that the cybernetic criminality profits are estimated at 750 billion EUR each year.

4. The Eurobarometer survey regarding cybernetic security in 2012 showed the fact that 38% of the internet users changed their behavior because of their concerns about cyber security: 18% are less likely to buy goods online, and 15% are less likely to use online banking services. The survey also showed that 74% of the interviewees agreed with the fact that the risk to become a victim has risen, 12% of them have already been a victim of online fraud, and 89% avoid sharing personal information.

5. According to the public survey regarding security and information networks, 56,8% of interviewees suffered last year incidents in this domain, with a severe impact on their activities.

6. At the same time, the Eurostat numbers show that until January 2012, only 26% of the European companies have defined in a formal way a security protocol in IT&C.

2. Priorities and strategic actions

EU needs to safeguard an online environment that offers the highest possible level of freedom and security towards everyone's benefit. Acknowledging the fact that approaching the security challenges of the cybernetic space is the responsibility of the member states, this strategy proposes specific actions that can improve the global EU performance. These actions are planned for both short-term and long-term. It includes a series of political tools and involve various parties from EU institutions to member states and the domain industry. The EU vision, presented in this strategy, is contoured around the five strategic priorities and approach the challenges mentioned above:

1. Creating cybernetic resilience; In order to promote cybernetic resilience in the EU, both authorities and the private sector must develop their capacities and cooperate in an efficient manner. Starting from the positive results obtained through the activities conducted until now, and continuing to do so on a EU level can especially help fighting transboundary cybernetic risks and threats, contributing to contouring a coordinated response in emergency situations. This will represent a strong support towards the proper functioning of the domestic market and it will improve the EU internal security.

2. Drastic reduction of cybernetic criminality; Cybernetic criminality is a form of criminality with one of the fastest growth rate, with more than a million individuals becoming victims each day. Cybernetic criminals and cybernetic criminality networks are becoming more and more sophisticated and we need to own the operational tools and capacities to approach them. EU and member states need a solid and efficient legislation in order to counter cybernetic criminality.

3. Development of policies and defense capabilities regarding the Security Policy and Defense Policy. EU efforts in the field of cybernetic security also implies cybernetic defense. In order to improve the resilience of information systems and communications that support interests regarding the national defense and security of member states, developing cybernetic defense capabilities should concentrate on detection, reaction and reverting to the state of normality after the sophisticated cybernetic threats.

4. Developing industrial and technological resources regarding cybernetic security; Europe benefits from excellent research and development capabilities, but many of the world leaders that provide innovative products and services in IT&C are outside the EU space. There is a risk that Europe will become extremely dependent not only of IT&C products but also of security solutions developed beyond its borders. It is essential that the hardware components and software products produced in the EU and tertiary countries, that are used more and more for services and critical infrastructures for mobile devices are guaranteed to be trustworthy, safe and that they provide private data protection.

5. Establishing an EU coherent international policy regarding cybernetic space and promoting fundamental EU values. Maintaining a free, open and secure cybernetic space represents a worldwide challenge that EU should approach with its partners and the relevant international organizations, private sector and the civil society. With its international policy regarding the cybernetic space, EU will try to promote internet openness and freedom, encourage development efforts of rules of conduct and apply the existing international legislation in the cybernetic space.

EU cybernetic strategy sets the prevention and reaction strategy towards disruptions and attacks that affect the European telecommunications network.

The directive proposes imposing a minimal level of security for the technologies, networks and digital services in all member states. This also means that some companies and organizations should have the obligation of reporting significant cybernetic incidents. The list includes search engines, cloud-type service providers, social networks, public administrations, online payment platforms such as PayPal and major commerce sites, such as Amazon.

Ways of insuring a high level of security for networks and information

The EU cybernetic security strategy establishes that EU's approach is the best way to prevent and react to disruptions and cybernetic attacks. The strategy presents a series of actions in order to consolidate the cybernetic resilience of information systems, reduce cybernetic criminality and consolidate EU's international policy regarding cybernetic security and defense.

The directive regarding network and information security (NIS) is an important element of the cybernetic security strategy. This means that EU member states, main internet service providers and infrastructure operators, such as electronic commerce platforms, social networks and transport services, bank services and healthcare services guarantee a safe and trustworthy digital environment all across the EU. Taking into consideration the fact that the approach used now is reliant on volunteers, the national capacities and the degree of implication and knowledge of the private sector varies considerably from one state to another. The directive aims to create equitable competition conditions by introducing harmonized norms that should be applied in all of the EU member states. The proposed measures include:

- The request that EU member states will adopt a strategy regarding NIS and will designate a national NIS authority that will benefit from adequate resources in order to prevent, manage and solve NIS risks and incidents.
- Creating a cooperation mechanism between the member states and the commission in order to send early warnings regarding risks and incidents, trade information and counter NIS threats and incidents.
- The request for certain societies and digital services to adopt risk management practices and report major information security incidents to the national security authority.

The request of reporting information security incidents aims to develop a culture of risk management and to make sure that the information is shared between the public and private sectors. The request includes:

- Critical infrastructure operators from certain fields, such as financial services, transportation, energy and healthcare.
- Information services companies, including application stores, electronic commerce platforms, internet payment platforms, cloud computing platforms, search engines and social networks.
- Public administrators

Conclusion

Present information systems can be severely affected by security incidents, such as technical difficulties and viruses. These types of incidents, usually called information and network related incidents, are becoming more and more frequent and more difficult to approach.

Many companies and governments from across the EU rely on infrastructures and digital networks to provide essential services. This means that when there are NIS related incidents, they can have a huge impact by compromising services and interrupting the activity of companies. Additionally, with the development of EU's internal market, numerous networks and information systems are functioning beyond the borders. A NIS related incident in a country could have effects felt in other countries and even the whole EU. Also, security incidents undermine the consumer's trust in online payment systems and information networks.

By introducing additional risk management measures and a systematic incident report measure, the directive allows information system dependent sectors to be more viable and stable.

The NIS objective is to insure a trustworthy and safe digital environment in EU. Citizens and consumers will have more trust in the technologies, services and systems on which they rely daily. This trust will be represented into a more inclusion favorable cyberspace and a digital economy which is growing fast, helping with economic stabilization. Governments and companies will be able to rely even more on networks and digital infrastructure in order to provide essential services domestically and transboundary. Safer electronic commerce platforms could attract more clients and could create new opportunities. IT&C security service and product providers will also benefit because of the increase in the need for their products. EU economy will benefit because sectors that rely heavily on NIS will be better supported for offering a viable service.

References:

1. Rule No. 6/2015 on the management of operational risks caused by the computer systems used by the government entities, authorised/approved and/or supervised by the Financial Supervisory Authority.

2. http://www.consilium.europa.eu/ro/press/press-releases/2015/06/29-network-information-security/