The 12th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 9th-10th 2017

TACKLING CYBER ATTACKS IN THE EUROPEAN UNION

Professor Ileana TACHE, Ph.D.*
Scientific Researcher Lavinia DOVLEAC, Ph.D**

***** Transilvania University of Brasov/ Faculty of Economic Sciences and Business Administration/ Brasov/ Romania
**Transilvania University of Brasov/ Faculty of Marketing/ Brasov/ / Romania

Abstract:
Cyberattacks affect both individuals and companies and the damages have a long term effect. Companies in the European Union (EU) are spending more to safeguard their digital assets, but cybercrimes are still growing in frequency and severity. What's needed now isn't more security, but better security. The unprecedented cybercriminal activity is generating so much cyber spending, it's become nearly impossible for analysts to accurately track. Many corporations are hesitant to announce breaches they've suffered and the amounts of their increased security budgets, for fears of reputational damage and of antagonizing cybercriminals. The aim of this paper is to highlight the necessity for EU companies to protect better from cyber attacks by investing more in consulting services, protection services, cyber insurance. The objectives of this paper are: to perform an evaluation of the problems faced by the organisations because of cyber attacks and to offer some solutions for cyber protection – linked to the EU policies in this field.

Key words: cybersecurity policy, sybermarket, cyberattacks,

1. Introduction

Equal opportunities to develop knowledge-based information society and risks to its functionality [1]. Through its characteristics, the cyberspace offers free access to information and communications, and also represents a favourable environment for threats, vulnerabilities or incidents for the security of people and goods. From the perspective of the gravity of risks and threats, cybersecurity is seen as an important component of national security [2].

By Government Decision no 494/2011 for the Establishment of the Romanian National Computer Security Incident Response Team – CERT-RO, cybersecurity is considered "the state of normality following the implementation of a set of proactive and reactive measures ensuring the confidentiality, integrity, availability, authenticity and non-repudiation of the information in electronic format, of public or private resources and services in the cyberspace. The proactive and reactive measures can include: policies, concepts, security standards and guides, risk management, instruction and awareness-raising, implementation of technical solutions to protect cyber infrastructures, identity management, consequences management" [3].

Cybersecurity includes non-computer devices and non-IT centric platforms and environments which covers entire sub-markets like aviation security, automotive security, IoT security, and Industrial Internet of Things (IIoT) security. All these market segments combined make up the cybersecurity market.

At the EU level, the adoption a European cybersecurity strategy, aimed at harmonizing the efforts of Member States to address security challenges in cyberspace and critical information infrastructure protection, is still work in progress [1].

The rapidly evolving nature of cyber threats has required the adoption, including at NATO,

of a new concept and a new cyber defense policy. To this end, NATO has redefined its role and area of action in the field and developed a plan of action to develop the capabilities required to protect own cyber infrastructure own and mechanisms for consultation

between Member States and for assuring assistance in the event of major cyber attacks.

The average number of attacks against any company's set of web applications is very high. They range from 300 to 800 dayly and never fall below 140. These attacks aim to harm government entities, financial services companies, IT companies, educational and healthcare institutions, or energy and manufacturing companies [6].

This paper highlight the importance of cybersecurity for the European Union countries, considering the existing cybersecurity policies, the evolution of cyberattacks on companies and the possible cyberprotection solutions and the cybersecurity strategies applied by Romanian companies.The aim of this paper is to highlight the necessity for EU companies to protect better from cyber attacks by investing more in consulting services, protection services, cyber insurance. The objectives of this paper are: to perform an evaluation of the problems faced by the organisations because of cyber attacks and to offer some solutions for cyber protection – linked to the EU policies in this field.

2. Cybersecurity policies from the European Union perspective

Figures will be numbered as follows: Cyberspace is an intrinsic part of the development of any country. A strong information and cyber capacity is crucial for the region to progress and develop in the economic, political and social spheres.

Many nations are concerned about issues such as critical infrastructure protection, fighting cybercrime and promoting good governance. But even those nations that favor a state-centric approach to cybersecurity have noted the important roles that the international community and international law play in enhancing cybersecurity [4].

The cybersecurity policymaking is challenging because of various factors: Intangible nature (The impact of cybersecurity breaches is often not visible in a physical sense), Socio-technical dependence (humans are the weakest link in the cybersecurity chain), ambiguous impact (what impact will there be if data is stolen or altered), Contested nature of fighting cybersecurity (uncertainty about the measures that need to be taken to improve security) [16].

Many countries have adopted national cybersecurity strategies and related legislation, taking into account both security and freedoms. South-Eastern Europe, and especially the Western Balkans, is lagging behind [17].

The main pieces of EU legislation used in fighting cybercrime are presented in the table below.

Year of approval	**Type of EU document**	**Specifications**
2010	The Digital Agenda for Europe (DAE)	the shared understanding that trust and security are fundamental preconditions for achieving the objectives of the 'smart growth' dimension of the Europe 2020 Strategy.

2013	The EU Cybersecurity Strategy	the EU's first comprehensive policy document in this area
2014	the EU Cyber Defence Policy Framework	one of the main documents with respect to the development of cyber defence capabilities
2015	The European Agenda on Security (EAS)	provide the overall strategic framework for the EU initiatives on cybersecurity and cybercrime
2015	the Digital Single Market Strategy for Europe	In order to catch up with the additional technical innovations and policy challenges emerging in the years of the development and adoption of the DAE
2016	The directive on network and information security (NIS)	requires each member state to establish a Computer Security Incident Response Team (CSIRT) and sets up a cross-EU cooperation group for strategic cooperation

Source: [17]

2.1 Case of Romania

The Romanian state assumes the role of coordinator of cyber security activities at national level, in line with European Union (EU) and North Atlantic Treaty Organisation (NATO) initiatives. Romania adopted its national cyber security strategy in 2013, setting out the objectives and principles for understanding, preventing and counteracting cybersecurity threats, ulnerabilities and risks. In the same year, Romania established a Cyber Security Research Centre (CSSIR; English) in order to promote, support, implement and coordinate security research in IT security inside the country, and also conduct international actions through short-, mid- and long-term partnerships on cyber security [1].

In May 2017, the Romanian Intelligence Service (SRI) organised its first national cyber security exercise called CyDEx17 [7]. The exercise was aimed at testing and assessing the way of managing the cyber incidents, the institutions' response at operational level (tactically and strategically), while seeking to provide appropriate security levels across the cyber infrastructures and to optimise co-operation across institutions by identifying and limiting the impact of such incidents [8].

Romania aims to develop both a dynamic information environment based on interoperability and specific information society services. In this respect, there is a need to develop a cybersecurity culture among the ITC users, which are often insufficiently informed of potential risks and countering solutions.

The purpose of Romania's cyber security strategy is to define and maintain an secure virtual environment, with a high degree of resilience and confidence, based on national cyber infrastructures. This strategy would constitute an important support for national security and good government, to maximize the benefits for citizens, businesses and the Romanian society as a whole.

Developing the cooperation between the public and private cyber security purposes is a priority for action in international bodies or alliances to which

Romania is part, given that cyberspace brings together both cyber infrastructure owned and operated by state and private entities.

3. The evolution of cyberattacks on companies and cyberprotection solutions

Most companies are highly dependent on digital processes and this dependence will continue to increase. A one-hour business interruption can result in financial losses ranging from €100,000 to €3 million – depending on the company's size and how seriously critical business applications are affected [5].

Over half a billion personal records were stolen or lost in 2015 [9] and more than 4 billion data records were stolen globally in 2016 [10]. Businesses were the prime targets, with more than half (55%) of the reported breaches but hackers also attacked medical institutions and government agencies. It was reported a concerning increase in the number and sophistication of phishing attempts, targeting specific departments within organizations. While some phishing attempts may seem obvious, such as a fake delivery tracking emails, the Legal and Finance departments at some company were targeted with well-crafted phishing attacks.

There were identified more than 430 million new unique pieces of malware in 2015, up 36% from 2014. Vulnerabilities can appear in almost any type of software, but the most attractive to targeted attackers is software that is widely used. Again and again, the majority of these vulnerabilities are discovered in software such as Internet Explorer and Adobe Flash, which are used on a daily basis by a vast number of consumers and professionals.

The performance of organizations in the field of cyber security must address a number of issues, such as [11]: data collection (in an environment characterized by frequent changes), the quality of information (under explicitly uncertain conditions), the quantification of performance qualitative parameters or intangible results (e.g. innovation and adaptation capacity), the inclusion of sensitive data (ethical and legal barriers).

IT and cybersecurity ar often times not on management's agenda until a crisis occurs and doesn't receive the required attention until it's already too late. We're also in a field that is rapidly changing. Every day thousands of new viruses and malware programs are detected. Even experts have trouble keep ing up with the latest technology.

3.1 Cybersecurity and IT services spendings

In 2004, the global cybersecurity market was worth $3.5 billion and in 2017 it is expected to be worth more than $120 billion. The cybersecurity market grew by roughly 35X over 13 years.

Specialists predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the next five years, from 2017 to 2021 [13]. Also, cybercrime will continue rising and cost businesses globally more than $6 trillion annually by 2021. The cybercrime cost prediction includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

3.2 IT services spendings inside companies

Consulting and IT outsourcing are currently the largest categories of spending on information security. Until the end of 2020, the highest growth is expected to come from security testing, IT outsourcing and data loss prevention (DLP). By 2018, 90% of

organizations are expected to implement at least one form of integrated DLP, up from 50% today [14].

Organizations have been deploying DLP to address regulatory compliance, intellectual property (IP) protection and data visibility and monitoring. Newer solutions that include user entity and behavior analytics, image analysis, machine learning, and data-matching techniques are being used to augment existing solutions.

The unprecedented cybercriminal activity is generating so much cyber spending, it's become nearly impossible for analysts to accurately track.

Even IT security services are difficult to fully size. Tech is a cottage industry which includes tens of thousands of VARs (value-added-resellers), IT solution providers, and SIs (systems integrators).

3.3 Cyber insurance

Companies are trying to manage the cyber risks by adopting a cyber insurance program covering specific losses. Insurance solutions have been brought to market by innovative insurers. In time, cyber risk will support a vibrant new insurance market. For insurers, barriers to offering more economical coverage include the lack of claim history to use in pricing, and a hard to quantify clash potential.

Coverage is available from many insurers for various aspects of cyber risk covering both first party and third party losses. Typically third party coverages include: Regulatory Investigation Expense, Breach or Loss of Data, Media Liability. First party coverages include: Crisis Management Expenses, Breach of the Network, Extortion and Business Income and Extra Expense [12].

While the European market for IT insurance is still developing, many companies in the United States already have liability policies covering data loss. This is because US companies are required to inform their customers about security breaches. The introduction of similar regulations is currently being discussed in EU member states including the UK [5].

4. Cybersecurity strategies in Romanian companies

Companies might be reluctant to share information on their cybersecurity spending with the public. The paradox is that too little spending might indicate a weak protecion, while too much spending might indicate too much concern that they might be the potential target of attacks [16].

Investments in cybersecurity are mostly driven by regulatory requirements instead of the organizations awareness of the actual and ongoing IT security threats. According to the results of a survey launched recently, "Security in the Digital World" [15], 57% of the organizations responding to this survey are planning to increase their cybersecurity budget in the next financial year, with 20% counting on maintaining the current spending level, while 23% still don't not have a clear picture as to their next year's budget.

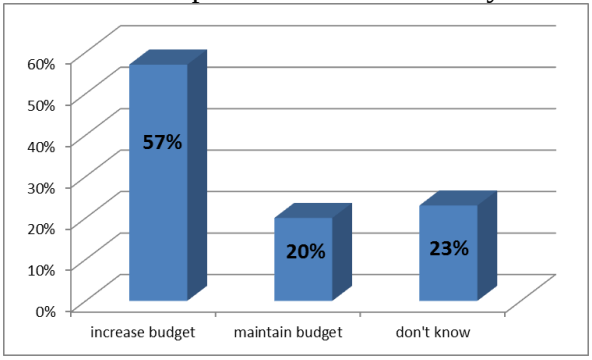

Fig.1. Managers intentions for cybersecurity budget

With 40% of the surveyed companies not having a formal cybersecurity strategy, and only 10% having reached a maturity level where the strategy is defined, implemented and optimised, the study reveals the fact that information security is not yet fully understood and supported at Board of Directors level.

In terms of perceived cybersecurity challenges, 87% of respondents declared that they are preoccupied with potential data leaks, 73% worry about malware (including ransomware), 70% are concerned about potential disruptions in business continuity, with another 70% preoccupied to ensure protection against targeted attacks.

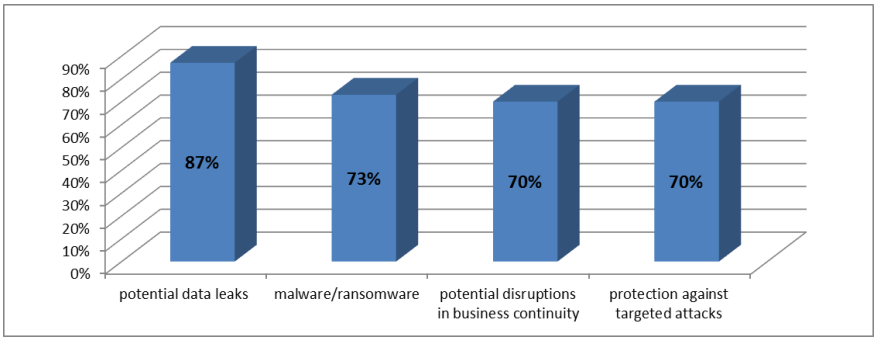

Fig.2. Cybersecurity challenges for Romania companies

As for the potential factors that could have a positive effect on cybersecurity, vast majority of respondents considered that increasing awareness (including training) of the employees regarding threats combined with increasing awareness and support of the management board are critical factors to improve digital security. Another positive factor is considered the enforcement of regulatory requirements as a major driver to improve digital security (77%). The need to hire additional security resources (67%) and to exchange security information with others (57%) were also considered by the large majority of respondents very important to improve digital security. Most of respondents would invest in data backup / recovery process (20%), improving access management to systems (19%) and data leak prevention solutions (16%).

5. Conclusions

The fact that companies are increasingly choosing to hold back critical details after a breach is a disturbing trend. Transparency is critical to security. While numerous data sharing initiatives are underway in the security industry, some of this data is getting harder to collect.

Manufacturers need to prioritize security and find the right balance between innovation, ease-of-use, and time-to-market constraints. Fundamentally, companies and consumers need to be assured that suppliers are building security into the IoT devices they are buying.

Website security encompasses more than the information in transit between a server and visitors to a website. Organizations need to think about their websites as parts of an entire ecosystem that needs constant care and attention if they want to retain people's trust and confidence. Website owners still aren't patching and updating their websites and servers as often as perhaps they should.

Managed detection and response (MDR) is growing as organizations are challenged to use both technology and human expertise to pinpoint risks and maintain a safe cyber

environment. This is especially relevant in addressing insider threats and targeted advanced threats.

The growing number of national cybersecurity strategies is a welcome development, but these documents still remain compromised by a number of significant issues. Future strategies or updates must not neglect human resources, specifically the awareness raising and education of government employees, which act as a first line of defense against potentially devastating cyber attacks [4].

References:

[1] *Cyber security strategy of Romania*. Available online at https://cert.ro/vezi/document/NCSS-Ro [accesed 12.09.2017]
[2] Mâță, D.C. (2015). Cybersecurity – Dimensions of national security, *Journal of Law and Administrative Sciences*, Special Issue/2015, pp.132-142. Available online at http://jolas.ro/wp-content/uploads/2015/07/jolas_sia14.pdf [accesed 20.09.2017]
[3] Published in the Romanian Official Gazette, Part I, no. 388 of 2 June 2011.
[4] Shackelford, S.J., Kastelic, A. (2016). *Toward a state-centric cyber peace?: analyzing the role of national cybersecurity strategies in enhancing global cybersecurity*. Available online at http://www.nyujlpp.org/wp-content/uploads/2016/01/Shackelford-Kastelic-State-Centric-Cyber-Peace-18nyujlpp895.pdf. [accesed 20.10.2017]
[5] *Attacks from cyberspace*, Available online at http://www.agcs.allianz.com/assets/PDFs/GRD/GRD%20individual%20articles/It_failures_cybercrime.pdf. [accesed 15.10.2017]
[6] *Web Application Attack Statistics: Q2 2017* (2017). Available online at http://blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html. [accesed 15.10.2017]
[7] Premieră la SRI: exercițiu național de securitate cibernetică - CyDEx17. Available online at http://www.economica.net/premiera-la-sri-exercitiu-national-de-securitate-cibernetica-cydex17_137809.html. [accesed 17.10.2017]
[8] National cyber security strategy - NIS Capacities. Available online at https://www.cyberwiser.eu/node/830/pdf. [accesed 17.09.2017]
[9] Symantec (2016). *Internet Security Threat Report* (vol.21). Available online at https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [accesed 17.10.2017]
[10] RsikBased Security (2017). 2016 Reported Data Breaches Expose Over 4 Billion Records. Available online at https://www.riskbasedsecurity.com/2017/01/2016-reported-data-breaches-expose-over-4-billion-records/ [accesed 22.10.2017]
[11] Cioacă, C., Bratu, A., Ștefănescu, D. (2017). The analysis of benchmarking application in cybersecurity. *Scientific Research and Education in the Air Force – Afases 2017*. Available online at http://www.afahc.ro/ro/afases/2017/8-M&H-CioacaCatalin,BratuAlexandru,StefanescuDaniel.pdf [accesed 23.10.2017]
[12] Propertycasualty360 (2017). The cyber liability insurance market rises. Available online at http://www.propertycasualty360.com/2017/09/19/the-cyber-liability-insurance-market-rises?slreturn=1510060332 [accesed 23.10.2017]
[13]Cybersecurity Ventures (2017). *Cybersecurity Market Report.* Available online at https://cybersecurityventures.com/cybersecurity-market-report/ [accesed 14.10.2017]
[14] Gartner (2016). *Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016.* Available online at https://www.gartner.com/newsroom/id/3404817 [accesed 14.10.2017]

[15] OusourcingToday (2017). *More than half of Romanian companies plan cybersecurity budget increase.* Available online at http://www.outsourcing-today.ro/articol.php?id=7084 [accesed 21.10.2017]
[16] de Bruijn, H., Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34 (1). Available online at http://www.sciencedirect.com/science/article/pii/S0740624X17300540. [accesed 02.10.2017]
[17] Diplo (2016). *Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities.* Available online at https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf . [accesed 02.10.2017]