INNOVATION AND THE EVOLUTION OF CYBER SECURITY TOOLS

Dumitrescu Mihaela-Sorina (author for correspondence)**,** Bucharest University of Economic Studies**,** Romania, sorina.dumitrescu16@yahoo.com
Paraschiv Dorel, Bucharest University of Economic Studies, Romania, dorel.paraschiv@ase.ro
Nițu Maria, Bucharest University of Economic Studies, Romania, nitumaria2@gmail.com
Florea Oana, Bucharest University of Economic Studies, Romania, oana.stefanescu@stud.ase.ro

We suggest you to cite this article as:
Dumitrescu, M.S., Paraschiv, D., Nițu, M., Florea, O. 2020. Innovation and the evolution of cyber security tools. *Junior Scientific Researcher*, Vol VI, No. 1, pp. 64-71.

Abstract

Virtualized offline services are available at remote locations all over the world, due to digitization which has conquered the world of information. Considering the unstoppable evolution of technology, new challenges for cybersecurity appeared. Traditional security solutions are not facing the complicated threats of new technologies anymore. Cybersecurity is not anymore about the protection of an individual device against ransomware or a basic attack. Certainly, to protect against cyber-attacks become more and more difficult than a decade ago. It supposes the protection of the virtual resources and of the entire networks.

Considering innovation and high tech vectors, the first objective of this article is to present the evolution of cybersecurity tools. The hypothesis of the article is that high tech favors cyberattacks, without a strong cybersecurity policy adopted by companies and governments. Cyber-attacks have the power to destabilize governments or political systems and to increase the risk of external and internal conflicts. If the security policy is not adapted to the market, companies risk a lot because they can lose all – business performance, money or brand perception.

Keywords*: cyber-attacks, cyber market, cybersecurity, digitization, high-tech, innovation*
JEL Classification*: O32, O33, K24*

Introduction

Cybersecurity represents a decisive topic for society and for businesses nowadays. Innovations, digitization and high technologies lead our lives, and these new technologies drive the organizations. This is the reason why the risks of cybersecurity attacks become more and more threatening. Technology is always evolving due to innovation. Newer technology is constantly leaving back older technology. Digitization has conquered the

world of information and of virtualized offline services which are available at remote locations all over the world. Therefore, new challenges for cybersecurity appear with the unstoppable evolution of technology.

Nowadays, we can not speak about cybersecurity just for the protection of an individual device against ransomware or a basic attack because it evolved to the protection of the virtual resources and of the entire networks. Traditional security solutions are not facing the complicated threats of new technologies anymore.

Cybersecurity does not represent a new concept but gains more and more importance. Companies invest a lot in technology which drives their outcomes, but at the same time, it may have disastrous consequences caused by potential attacks. Thus, security gains a higher priority in companies.

Digital transformation is leveraged by companies and impacts the use of the security, which is linked to business objectives through disruptive business models like mobile banking. In this way, the focus on the cyber threats is strengthened.

Background

The concept of security of digital assets is not new. From the 1950s, government agencies felt the potential risks caused by using computers and established the United States Communications Security Board and The National Security Agency. According to cpomagazine.com (2019), the global spending for cyber security is estimated at $10 billion, by 2027. It is essential to realize how important is cyber security and its threats for the Internet of Things (IoT) world, where internet is a must-have for daily activities, using devices like smartwatches for the control system of homes, cars or smart TVs.

According to the same source - cpomagazine.com (2019), Global Market Insights estimated that the industry of cyber security would reach $300 billion by 2024, growing exponentially like technology. Also, Forbes estimated that it will be spend $6 trillion for cyber security, much more than cost the natural disasters or the illegal drugs traffic in one year.

Citing the website cpomagazine.com (2019), a social media website is accessed every 15 seconds, around the world. One business will fall every 14 seconds because of ransomware attacks (Morgan, 2019). One malicious email from 302 will be received by public administrations, being a significant probability for tricking employees (O'Brien, 2017). Another real fact is that one IoT device may be easily attacked in the first 5 minutes of the internet connection. In this context, 61% of companies reported in 2018 minimum one cyber event, compared to 45% in 2017. Moreover, the cost of cyber-attacks is rising.

Cyber-attacks have the power to destabilize governments or political systems and to increase the risk of external and internal conflicts. Cyber is on the top 5 likely risks and on the top 10 fullest of impact risks. (Collins, 2018).

Cyber-defence and cyber-security represent two crucial pillars for the European Union in order to contribute to security and prosperity. EU is one important cyber player which protects its economy and its democratic principles. One example could be the

initiative of French President, launched in November 2018, who proposed having international norms for cyber threats. It was named the Paris Call, representing a declaration for the cooperation in cyberspace, being approved by 64 countries, universities, NGOs and private companies.

Main reasons for cyber-attacks are money and espionage (Verizon, 2019). Small and medium-sized firms are the main targets of the attacks. Bitkom, the German association from the cyber industry estimated €43 billion damage for German companies which were victims of sabotage and data espionage in 2017. On the other hand, the Department for Digital, Culture, Media and Sport of UK government identified in 2019 a lower percentage of companies which have been victims of a cyber-attack – only 32% relative to 43% for 2018, due to the newest cybersecurity measures adopted by companies as a response for GDPR - the newest data privacy law from the EU. (Wolff, 2019)

Because of digitization, organizations transform, and a critical part of the process must be security. Nowadays, it is not enough to set one network perimeter firewall for protecting against cyber-attacks. Our virtual world becomes varied, and the way of protection must be adapted. New technology transforms security operations in one industry. This industry offers a diversified range of products and services which help to fight against cyber-attacks.

Methods

The first objective of this article is to present the evolution of cybersecurity tools, considering innovation and high tech vectors for their evolution, expanding theoretical frameworks. **Secondly,** it will be presented the importance of adopting an adequate cyber security policy for companies in the context of digitization.

The **hypothesis** which will be tested is that high tech favors cyberattacks, without a strong cybersecurity policy adopted by companies and governments. It was used quantitative analyze for the theoretical research of specialized articles. The first step was to understand the effects of digitalization in order to identify the challenges of cyber security.

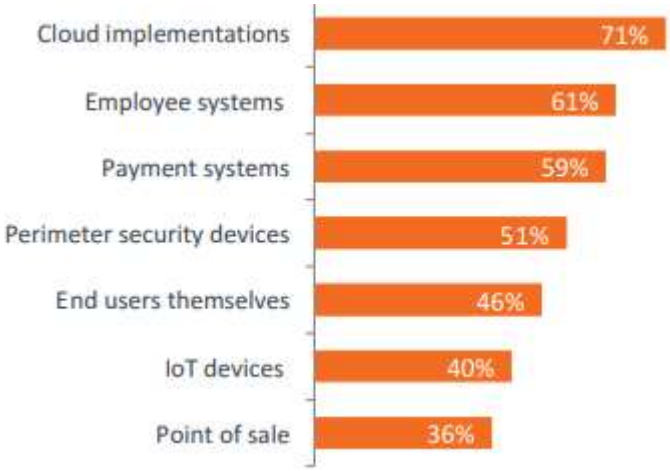
For presenting the importance of cybersecurity, it was analyzed the existing statically data of the European Commission. Then, the evolution of cybersecurity tools in the context of the new technologies like clouds, big data or Internet of Things, has been explained through synthesis.

Results and discussions, including research limits and advantages

New technology trends cause the change in the security domain. Initially, security was a secure perimeter, but advancing to the cloud technology imposed the security for data sets and discrete systems. Cloud solutions represent a threat for cybersecurity, next to employee applications like CRM, HR or payment systems.

From 2017, one area with the highest priority on cybersecurity is cloud technology, next to employee and payment system (Fig. No. 1).

Figure No. 1 Areas with high priority in the cybersecurity



Source: Comptia, 2017

Enterprises have chosen cloud architecture solutions, which apparently ease attackers' jobs because they have access to databases, virtual machines or clusters from one single place. Cloud vendors offer basic solutions for security, but companies should have security tools offered by third-parties which ensure the safety of their clouds.

For the payment system, a new solution was developed for preventing attacks in high-risk cases like online payments - two-factor authentication. It can include an OTP one-time password which is sent to one authorized device or biometrics. Using two-factor authentication decreases the risk of unauthorized access, together with employing monitoring tools for endpoint security which contribute to monitor the activity of the user and to report suspicious activity or emails to security teams. Also, there were developed tools using intent-based networking for ensuring security across the network.

Data from the cloud, from the mobile devices or the IoT devices, represent a potential cyber target. When we think at big data as very valuable information, it must be seriously protected against cyber-attacks. Having a huge volume of data, a security breach which allows access of cyber criminals could be disastrous. Also, we should consider big data a powerful weapon for fighting against cybercrime.

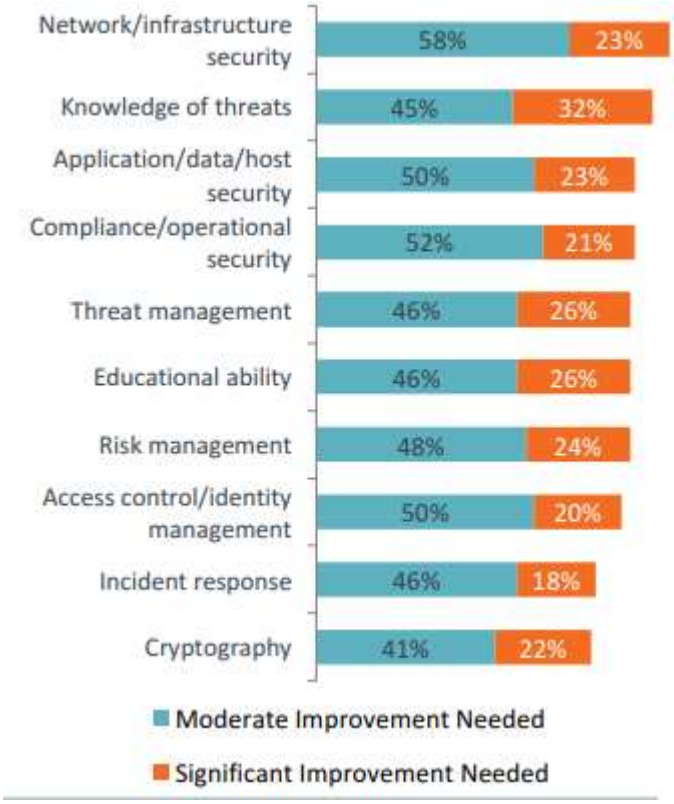
IT security does not represent a barrier for changing, which does not allow the implementation of innovative technologies or new processes. Security represents the core of the digital world, being a prerequisite for implementing new technologies. Security also offers 'speed of services', through SDN - software-defined networks which enable secured and broader access to data, being used for Internet of Things. Agility, speed, efficiency or acting smarter represent the IT security assets.

Companies can not afford an improper security approach. They must be careful and vigilant with the security of their applications and networks because attackers can be inactive for a long period before they decide to cyber-attack a system. Cyber risks become

more and more complex and impact all the critical issues like revenue, share prices, regulatory compliance or brand reputation. Traditional security practices protect against many risks, but the real cyber security challenges demand key capabilities like processes, people and technology, that must compose intelligent security. All of these suppose new security skills which have to be improved, for succeeding in ensuring cyber security.

The network infrastructure security must be continuously improved, together with knowledge of threats, application security or cryptography, which became nowadays mandatory skills (Fig. No. 2).

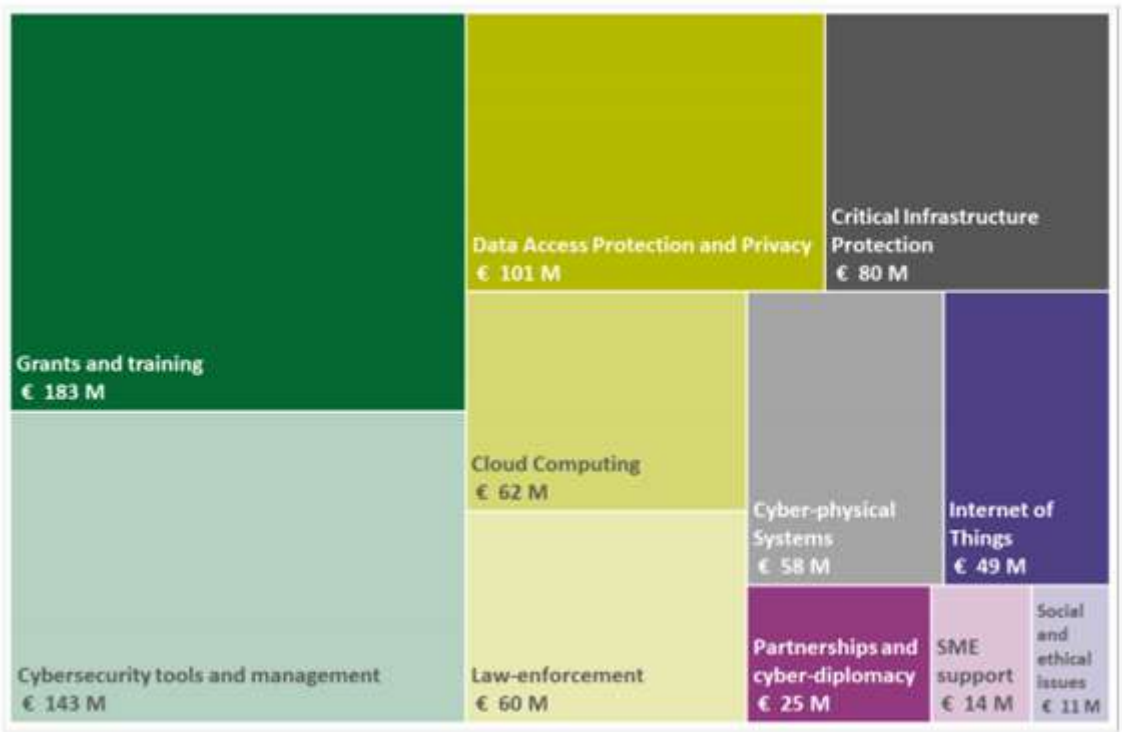
Figure No. 2 Top of improving security skills



Source: Comptia, 2017

For 2020, the European Commission contracted cybersecurity research projects for the management of cybersecurity, including newest technologies which may bring potential victims of cyber-attacks. The most significant amount was invested in training: €183 million, in research for cybersecurity tools: €143 million. Substantial amounts were invested for the newest technology: cloud €62 million or Internet of Things: €49 million (Fig. No. 3). *With these data, we can validate the hypothesis of the threat of cyberattacks for high tech, meaning that if companies and governments do not adopt a strong cybersecurity policy, high tech will favor cyberattacks.*

Figure No. 3 EU Cybersecurity research projects contracted for 2020



Source: ECA, 2019

This research shows **the evolution** of the cybersecurity tools and **its importance** in the context of the newest technologies. One possible extension of this research could be an applicative analysis of the effects of one efficient cybersecurity policy adopted by a high tech provider.

Conclusions

The cyber market is continuously changing, and companies must protect their networks against high-risk security threats. Indeed, to protect against cyber-attacks become more and more difficult than a decade ago. Companies risk a lot if they adopt a not trustworthy security solution because they can lose business performance, money or brand perception. The security policy must be adapted to the market.

Virtualization and digitization will evolve faster than today. The market is unpredictable, and we do not know what new technology will change the future. The digital world must have a standard of security which involves to gather, to synthesize and to analyze data. In this context, it is about what the data could offer us.

We can not predict how the industry will evolve, but we know that digitization and innovation will continue to grow exponentially, remaining crucial for succeeding. In the same time, cybercrime threat is increasing, and companies can not be reactive. Companies need to improve their security systems in order not to become the next victim.

In conclusion, companies have to make cyber security efforts for protecting against a range of challenges brought by new emerging technologies, like trends in social media, mobile usage, which cause potential attacks.

Acknowledgement

This work was cofinanced from the European Social Fund through Operational Programme Human Capital 2014 - 2020, project number POCU/380/6/13/125015 "Development of entrepreneurial skills for doctoral students and postdoctoral researchers in the field of economic sciences"

Bibliography

1. Comptia. (2017) The evolution of security skills. [Online] Available from: https://www.comptia.org/content/research/the-evolution-of-security-skills [Accessed: 2nd May 2020]
2. Collins, A. (2018) The global risks report 2018. World Economic Forum. [Online] Available from: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf [Accessed: 2nd May 2020]
3. Cpomagazine. (2019) 11 Eye Opening Cyber Security Statistics for 2019. [Online] Available from: https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019/ [Accessed: 2nd May 2020]
4. Disruptionhub. (2017) The Evolution of Cyber Security. [Online] Available from: https://disruptionhub.com/evolution-cyber-security/ [Accessed: 2nd May 2020]
5. ECA. Europa. (2019) Challenges to effective EU cybersecurity policy. [Online] Available from: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed: 3rd May 2020]
6. Informationage. (2018) Securing the future: The evolution of cyber security in the wake of digitalization. [Online] Available from: https://www.information-age.com/evolution-cyber-security-wake-digitalisation-123470747/ [Accessed: 2nd May 2020]
7. Morgan, S. (2019) Official Annual Cybercrime Report. *Herjavec Group*. [Online] Available from: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf [Accessed: 2nd May 2020]
8. Ninjarmm. (2019) 7 Eye-opening Cybersecurity Statistics every small-business needs to know in 2019. [Online] Available from: https://www.ninjarmm.com/blog/small-business-cybersecurity-statistics-2019/ [Accessed: 2nd May 2020]
9. O'Brien, D. R. (2017) Internet Security Threat Report. Email Threats. [Online] Available from: https://docs.broadcom.com/doc/istr-email-threats-2017-en [Accessed: 2nd May 2020]

10. Techgenix. (2019) Rising to the challenge: how cybersecurity has evolved to tackle new cyberthreats. [Online] Available from: http://techgenix.com/cybersecurity-cyberthreats/ [Accessed: 2nd May 2020]
11. Verizon. (2019) Data breach investigations report. [Online] Available from: https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf [Accessed: 2nd May 2020]
12. Wolff, G. B., (2019) Hybrid and cybersecurity threats and the European Union's financial system. [Online] No. 32349, Bruegel. Available from: https://www.bruegel.org/wp-content/uploads/2019/09/PC-10_2019.pdf [Accessed: 3rd May 2020]