Enhancing investment through cyber security policies – Case of Albania

Vilma TOMCO
Dr., *General Director of National Authority for Electronic Certification and Cyber Security, Tirana, Albania*
E-mail address: vilma.tomco@cesk.gov.al

Klorenta Janushi PASHAJ
Msc., *Expert at National Authority for Electronic Certification and Cyber Security, Tirana, Albania*
E-mail address: klorenta.janushi@cesk.gov.al

Abstract
Today the security of a nation state is not only restricted to its borders and sovereignty but it also extends to protecting against new borderless risks and threats. Globalization and the growth of an interconnected global environment through the Internet have brought immense societal benefits but have also opened up new venues for attacks and threats from governments, criminals, terrorists, private companies, and individuals. The emergence of actors from different locations, with different motives and the desire to challenge the rule of law and international order who can employ readily available tools and operate in a global cyber environment makes it incredibly challenging for nation states to successfully employ protective measures.In this article will be drawn a clear picture of the current situation of the cyber ecosystem in Republic of Albania. Then will be reviewed the investment of the private and public sector in the field of cyber security. At the end will be given recommandations stated in the Value section below.
Prior work In January 2017, was approved the law on Cyber Security and bylaws on Critical and Important Information Infrastructures. Since Albania is non-EU member state, the NIS Directive is not fully transposed in the law, but there is a good will between actors to improve the current cyber security situation.
Approach In order to capture the evidences in this article are used the methods of observation and case study of different information systems in Albania. Moreover, in order to analyze benefits of increasing the investment on cyber security, different cases from the region and Europe will be shown.
Results As information technology is developing rapidly, it is necessary to apply innovative, simple and secure methods, and increase investments in the cyber security field. In this article will be shown the real statistics of how the sectors have invests after the approval of the legal framework in Albania..
Implications This article contains implications for the groups of academics, who can use the statics and case studies in order to improve and update their lectures; for researchers who can take to another level the recommendations and for the practitioners who can update their knowledge on cyber security field in Albania.
Value This article gives recommandations for building a high protected information system or mechanism for raising the level of security of the information systems. It also contains guidelines for public administration and private sector for building resilience in cyber security ecosystem in Albania.

Keywords: cyber security strategy, resilience, trust.

1. Introduction
The Internet is one of the things humans have built that they don't truly understand[1]. Hundrens of millions of people are creating and consuming innumerable amount of digital content in an online world, which is not bound by terrestrial laws. As this virtual space grows larger, our understanding of nearly every aspect of life will change. Never before in history have so many people, from so many places, has so much power at their fingertips.

In the 21st century, life without Internet is unimaginable and at every level of society, connectivity will continue to become more affordable and practical in substantial ways. The vast majority of us will increasingly find ourselves being governed in two worlds at

one. The virtual life has become as important as, if not more than real life. Businessmen have capitalized on this raging internet obsession to not just advertise but also to scale their businesses.

Companies can have branches all across a country and still manage to have a centralized cloud system accessible to all the employees through a private network. In recent years the level of attention paid to cybersecurity issues by organizations has been increased potentially. Cyber risk is now a board-level issue and IT security budgets have been increased propotionally[2].

While companies are using all kinds of sophisticated technologies and techniques to protect critical assets, it is important to have in place a national baseline in legal terms for cyber security requirements.

Sections below elucidate the importance of investing in cyber security and the impact of national cyber security programs in enhancing investment and mitigating cyber risks. Below is described too the cyber security state of play in Albania, level of investment and policies in place.

1.1. Reasons to invest in cyber security

The vast majority of security failures occur due to misaligned incentives [2]. CISOs can only implement programs supported from the highest levels of the company.CEOs must not forget that there are certain perils involved in their daily life business tasks in the digital world [3]. Some reasons to incorporate cyber security into the businesses are listed below:

- Growing rate of Cloud data
  The amount of data generated increases with the business expansion. For ease of operation most companies back up their data in private cloud systems. The vast amount of sensitive information could result is a massive amount of financial loss if the back up is not protected properly.
- Employee errors
  This is yet another aspect which can make the business vulnerable to attacks. It isn't just important to adopt a policy and security measures. Moreover the company need to invest periodically in staff trainings.
- Harming reputation
  Cyber attackers thrive on catching the vulnerabilities in the system and bring the company to its knees. In this framework the companies should invent in protecting the assets from ransomware and other threats to protect their reputation.
- Advent of IoT
  Internet of Things has become the norm with centralized data systems being automated. By gaining access at any one entry point, hackers can infiltrate the entire system and gain access to all the company's private records, client information etc.

1.2. Cyber Security State of Play in Albania

Cyber security is a concept emerged with the use of information technology tools to protect computer systems from theft or damage to their hardware, software or electronic data, as

well as the interruption or misuse of the services they provide. Developments in new technologies like 5G and IoT are another reason to increase cyber security measures.

European countries emphasized this area through the development of a common regulatory framework that consists in the adoption of the Directive on Security of Network and Information Systems (NIS Directive) (2016/1148). Albania, as part of its engagement as a candidate for EU membership, has transposed this directive partially, through Law no. 2/2017 "On Cyber Security". The law entrusts the National Authority for Electronic Certification and Cyber Security (AKCESK) for its oversight and fulfillment with by-law acts, with a view to full implementation of the law. In fulfillment of this obligation, in June 2018, the entire regulatory framework has been completed. During the drafting of by-law acts, the Authority cooperated closely with the public and private sectors to identify critical and important information infrastructures, concretizing this work in the adoption of the Council of Ministers Decision No. 222, dated 28.04.2018 "On Approval of the critical and important information infrastructure list".

The operation of a National CSIRT is an essential component of a country's overall strategy for securing and maintaining vital technologies for national security and economic vitality. The National Authority for CESK operates in the capacity of the national CIRT pursuant to the Law no. 2/2017 "On cyber security". In order to fulfill the functional tasks, AKCESK has adopted a methodology for the organization and functioning of CSIRTs at the national level, which sets out the obligation to set up teams of CSIRTs (responsible groups for the management and handling of cyber incidents), systems which are managed by critical and important information infrastructure operators. The establishment of these teams affects all sectors in increasing security investment in information systems and networks that consist of:

- Establish dedicated security jobs positions (sectoral CSIRTs)
- Improve system functionalities by implementing additional measures to increase security levels and co-ordinate with national CSIRT for the real-time handling of cyber incidents
- Increase the technical and professional capacities of human resources, through ongoing specific training in the field of cyber security

Meantime, with the support of World Bank, it is done the evaluation of cybersecurity maturity level in Albania. The results that is presented in the below graph, make us aware to focus on two domains: a)Cyber security policy and strategy and b) Cybersecurity, education, training and skills, since we see that there are a lot to be done. And this was the focus of our study.

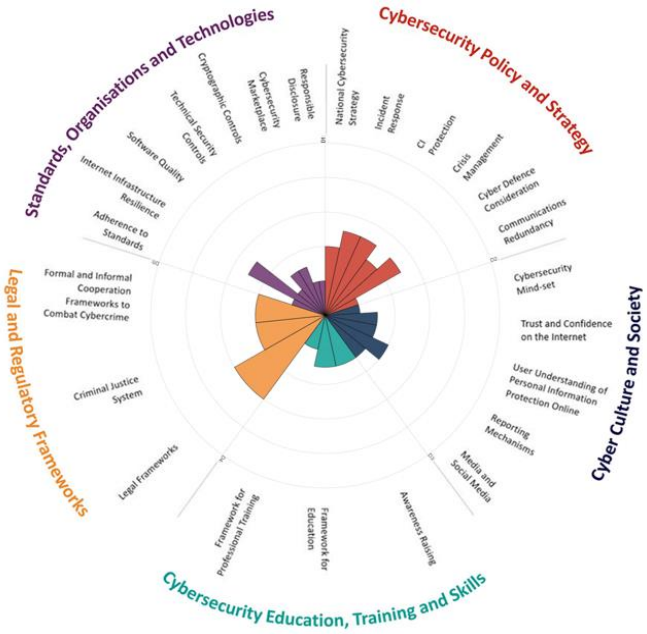

Fig. 1: Overall representation of the cybersecurity capacity in Albania [3]

2. Demand of the labour market in public and private sector

2.1. Introduction to Certification in Cyber Security

Cyber security is important for every area of activity, from government to corporations, from the military to the medical, financial and personal fields, because each one collects, stores and transmits data, most of which are sensitive information.

As the amount of digital data and transactions increases, there is a growing need for cyber security professionals in different roles. This has opened doors for a profitable career for IT professionals.

High labor market demand, salary, qualification opportunities, and ease of achieving qualifications, are a good reason to seek certification as cyber security professionals. The more certified professionals have a company, the higher the opportunities it has to protect assets from potential cyber attacks. The following table presents two security levels of companies according to the certifications owned by its employees.

Table 1. Certifications on cyber security

Types of certificates for medium security level	Types of certificates for a high level of security
Certified Information Systems Auditor (CISA) ofruar nga ISACA	Mobile and Web Application Penetration Tester
Certified Information Security Manager (CISM) ofruar nga ISACA	Global Information Assurance Certification Penetration Tester
ISO 27001	GIAC Exploit Researcher
ISO 9000	Offensive Security Certified Professional
ISO 20000	Ethical Hacking
Network+	Penetration Tester

Source: Authors

2.2. Labor market demand in the private sector

Sections below represent the current situation and organization of the IT and security departments of three of the largest sectors in the country: banking sector, insurance companies and hospitals.

The statistics were gathered from a survey of National Authority for Electronic Certification and Cyber Security.

2.2.1 Banking sector

In this sector were analyzed 7 banks that operates in Albania. From the analysis in the sector of these second tier banks, was found that all the banks have well-established infrastructure often associated with General safety information procedures. All the analyzed banks have their headquarters in Tirana and the branches in Albania's main districts.

The first bank analyzed, has 76 branches distributed throughout Albania with a staff of over 1200 employees. In this bank, the IT division has 78 employees divided into 5 sectors. Respectively:

- Sector of services and servers
- Development Sector
- Information Security Sector
- Information Management Sector
- IT Audit Sector

The second bank that was analyzed, has 40 branches distributed throughout Albania with a staff of over 660 employees. In this bank IT division has 48 employees divided into 5 sectors, respectively:

- Sector of services and servers
- Development and Reporting Sector
- Application Support Sector
- Sector of operations and administration
- Telecommunication and Network Sector

This bank does not have a dedicated sector related to the security of information systems. What is most noticed as a problem is the lack of staff certified with international well-known certificates.

The third bank analyzed, has 61 branches distributed throughout Albania with a staff of over 840 employees. This bank is the branch of the central bank in Turkey. In this bank, the IT division has 73 employees divided into 4 sectors, respectively:

- Banking and swift application sector
- Development Sector and IT Projects
- Sector of IT
- Sector of alternative distribution routes

What is worth mentioning is that the Audit Department is independent in this bank. The IT sector is also part of this department, but there is no technical security sector.

The fourth bank, has 58 branches distributed throughout Albania with a staff of over 640 employees. In this bank, the IT division has 20 employees divided into 2 sectors. respectively:

- Software sector
- Hardware sector

The security division at this bank is directly dependent on the bank's general director. However, the problem with the lack of certified staff with well-known international certificates remains the same here.

The fifth bank has 38 branches distributed throughout Albania with a staff of 320 employees. This bank is a branch of the central bank in Greece. At IT division there are 17 employees divided into 4 sectors. respectively:

- Application development sector
- Parameterization Sector
- Sector of IT networks and infrastructure
- Sector of IT Operations

It is worth noting that there is no information security sector and audit security sector. There is a lack of staff certified with well-known international certificates.

The sixth bank has 35 branches distributed throughout Albania with a staff of 580 employees. This bank is a branch of the central bank in Italy. In the IT division division there are 23 employees divided into 3 sectors. Respectively:

- Telecommunication Network Sector
- Development Sector and IT Projects
- Server and Service Sector

What is worth mentioning is that in this bank, the Information Security Audit Sector and the CISO Information Security Chief implement the ISO 27001 security rules and standards, and are present in the company's organizational chart. The bank meets ISO 27001 information security standards at an unsatisfactory level as it reaches 55-60%.

In the last bank analyzed, the Information Security Audit Sector and the CISO Information Security Chief implementing the ISO 27001 safety rules and standards are present in the company's organizational chart. The bank meets ISO 27001 information security standards at 80-83%.

In the Information Security sector, this bank covers the part of the information security technique through penetration testing, patching, log monitoring, and scanning of gates and DDoS cases. This staff has an elevated infrastructure but it is noticed that only 4 employees of the security unit within the security sector are dealing with these simulations and only

one employee is certified with international certifications such as Ethical Hacking at the Basic Level.

Meanwhile, international well-known certificates such as Mobile and Wet Application Penetration Tester, Global Information Assurance Certification Penetration Tester, GIAC Exploit Researcher, and Offensive Security Certified Professional are not available to employees employed as internal staff at this bank. This makes high security elements implemented by the central branch in France with their specialists.

2.2.2 Insurance Companies

In this section are analyzed the three largest insurance companies in Albania. The first company for the first time is implementing information security policies and has appointed an independent IT security chief from the IT department. However, there is no proper security department and its technical elements, and all penetration, monitoring and logging tests are carried out by an IT department composed of 7 employees. Meanwhile, from the aspect of auditing, the implementation of information security policies and their respective procedures are being implemented by the chief of information security. However, this company has not yet been certified according to ISO 27001.

The second company does not have information security policies and has not assigned any chief of information security. There is no proper security department and its technical elements and all penetration, monitoring and logging tests are carried out by an IT department composed of 5 employees. Meanwhile from the aspect of auditing the implementation of information security policies and their respective procedures are monitored by the central branch abroad.

The third company does not have information security policies and has not assigned any information security directors. The penetration, monitoring and logging tests are performed by the IT department consisting of 5 employees at baseline level. Meanwhile, from the aspect of auditing the implementation of information security policies and their respective procedures are not currently implemented in the company.

2.2.3 Private hospitals

In this section are analyzed the 3 largest hospitals in the country. The first and the second hospital analyzed have a department composed of two IT specialists. Currently, security policies and procedures are not applied. Access to the patient who manages the patients is realized through the username / password logon. Access to the software is realized through user privileges.

The third hospital has a department consisting of six IT specialists. In all the three hospitals, staff is trained on how to behave to handle confidential information, but more in-depth password training is needed.

3. Recommandations

To ensure the implementation of security procedures and to fulfill the role of CSIRT, the employees of the public and private institutions must be trained on how to react and deal with potential cyber incidents.

All systems and networks of institutions should be protected through the implementation of security measures, specifically critical and important information systems. All critical and important infrastructure at national level, both in the public and private sectors, should be identified.

For all critical systems in use, vulnerability / penetration tests should be carried out. After this process, the necessary measures must be taken to avoid the potential risks of attacks. All public and private institutions that have critical or important information systems identified or not, need to increase investment in human resources dedicated to the security of information systems and to add appropriate modules (hardware hardware) or software to increase their level of security.

All public and private institutions should build clear cooperation bridges with the National Authority for Electronic Certification and Cyber Security in order to build a safer online environment.

References

[1]Eric Schmidt, The new digital age : reshaping the future od people, nations and business. Introduction
[2]Moore, T., Dynes, S., Chang, F. (2016) *Identifying how firms manage cybersecurity investment*
[3]National Authority for Electronic Certification and Cyber Security https://cesk.gov.al/Publikime/2019/AlbaniaCMMReport.pdf
[4]Ross J. Anderson. (2001) *Why information security is hard - An economic perspective, pages* 358-365
[5]Hackernoon www.hackernoon.com 5 reasons why businesses should invest in cyber security.
[6]National Authority for Electronic Certification and Cyber Security www.cesk.gov.al