IT SECURITY IN ALBANIA: THE ROAD TO JOBS

PREPARED BY: IGLI TAFA

DECEMBER 2019

PUBLISHED BY RISI ALBANIA
A PROJECT OF THE SWISS
AGENCY FOR DEVELOPMENT
AND COOPERATION (SDC),
IMPLEMENTED BY HELVETAS AND
PARTNERS ALBANIA

RisiAlbania
Partner for Growth

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development
and Cooperation SDC

REPUBLIC OF ALBANIA
PRIME MINISTER'S OFFICE
DEPUTY PRIME MINISTER

HELVETAS Swiss Intercooperation | ALBANIA

PARTNERSALBANIA
FOR CHANGE AND DEVELOPMENT

Disclaimer: this version of the report has been modified to respect the confidentiality of respondents. The views and opinions expressed in this report are those of the author and do not necessarily reflect the official policy or position of the RisiAlbania project.

ACKNOWLEDGMENT BY THE AUTHOR:

I would like to thank all public and private institutions, part of this study, who worked closely with the accuracy of the information that is needed to present the situation, through measurable and factual components.

I would like to thank the National Authority for Electronic Certification and Cyber Security for co-operation and co-ordination of ideas and vision, which has influenced the quality of this study.

EXECUTIVE SUMMARY

The goal of this report is to make an assessment of the demand and supply of the labor market for cybersecurity skills and services, and to provide recommendations on how to improve labor market coordination. We analyze the situation of demand and supply of cyber security in Albania including 1. Public Universities; 2. Private Universities, and 3. Private training centers on the supply-side; and 1. Public Sector companies, and 2. Private Sector companies on the demand-side.

IT security curricula are not available in bachelor's degree courses on neither private nor public universities. The number of universities that have implemented IT security branches in professional / scientific master's degree is low: only two private Universities and one public University, meanwhile in the rest of universities IT security is just a module. Therefore, **universities and private training centers are offering a limited supply of IT security skills**. The labs in these institutions are far from being professional. There is a shortage of pedagogical staff to cover information security subjects and limited competence of pedagogues in these areas. The students attending information security programs are 60% - 40% men to women.

IT Security in public institutions is very weak. It is implemented mostly in National Agency for Information Society (NAIS), since all the public infrastructure is maintained and managed by this institution. This is the only institute which can deliver Public Key Infrastructure (PKI) for public and private subjects. Other public institutions have implemented some spots of security features, but still present vulnerabilities.

Our analysis of private companies includes: 1. Second Level Banks; 2. Insurance Companies; 3. Hospitals; 4. Other Manufacturers. Security implementation in second level banks is satisfactory both in technical aspects or organogram and management. Insurance companies have a beginner to moderate level of security in technical and human resources. IT security implementation in hospitals and other manufacturers is very poor in technical and human resources. With the implementation of the new cybersecurity law, banks will require more cybersecurity technicians and demand for qualified professionals will increase. In this section, we make an assessment on **what is the current number of cybersecurity professional in these sectors and what are forecasted numbers and qualifications needed**.

We assess the **investments for establishing a high security level system (hardware, software, human resources).** We also have developed the job profiles of the three main positions related to cybersecurity: 1. Information security technician; 2. Information Security Analyst; and 3. Information security auditor.

In our recommendations we propose to setup curricula in IT security at the level of master and private training centers that should include at least **two job profiles: IT security technician, and IT Security Auditor.** These will be the most demanded profiles in Albania and abroad.

List of Abbreviations

AKCESK - Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike

AED – Albanian Electronic Distribution, Kompania e Kasave Fiskale

ABI – American Bank of Investment, banke e nivelit te dyte qe operon ne Shqiperi

AlbControl – Instituti per menaxhimin e hapsires ajrore

ACL- Access Control Lists, Lista e kontrollit te aksesit

B2B – Business to Business, Menaxhimi i biznesit me nje biznes tjeter

B2C – Business to Customer, Maredhenia e biznesit me klientin

BKT – Banka Kombetare Tregtare, banke e nivelit te dyte qe operon ne Shqiperi

BCP – Business Continuity Plan, qe ka te beje me strategjine e vazhdueshmerise e sherbimeve te biznesit

CSIRT – Computer Security Incident Response Team, ngritja e nje skuadre per menaxhimin e incidenteve te sigurise ne nje ndermarrje

CESK - Certifikimin Elektronik dhe Sigurinë Kibernetike

CIRT - Computer Incident Response Team, ngritja e nje skuadre per menaxhimin e incidenteve te sigurise ne nje ndermarrje.

CIT - Instituti Kanadez i Teknologjisë

CISA - Certified Information Systems Auditor ofruar nga ISACA

CISM - Certified Information Security Manager ofruar nga ISACA

CISCO – Brandi i teknologjise bazuar ne Rrjetat dhe pajisjet e sigurise se informacionit

CISP - Certified Information Systems Security Professional, ofruar nga ISACA

CRISC - Certified in Risk and Information Systems Control, ofruar nga ISACA

COMPTIA - Computing Technology Industry Association, kompania nderkombetare per certifikimin e pajisjeve elektronike

CERT-CSIH - CERT-Certified Computer Security Incident Handler

CGEIT - Certified in the governance of enterprise IT

CIA – Konfidencialitei/ Integriteti/ Disponueshmeria

CCNA – Cisco Certified Network Association, certifikata per njohurite bazike ne rrjet, leshuar nga kompania Cisco

CCNP Security - Cisco Certified Network Professional, certifikata per njohurite profesionale ne rrjet, leshuar nga kompania Cisco

COBIT - Eshte nje framework krijuar nga ISACA per menaxhimin e informacionit dhe drejtimin e saj.

CISSLP - Certified Secure Software Lifecycle Professional eshte nje certificate nga $(ISC)^2$ qe fokusohet ne aplikimin e sigurise brenda ciklit te zhvillimit te software-t.

CyberSecurity – Ekspert i Sigurise se Informacionit, bazuar kryesisht ne ndertimin e strategjive mbrojtese ndaj krimit kibernetik

DDoS – Distributed Denial of Service

DRP – Disaster Recovery Plan, Plani per rinisjen e sherbimeve ne nje vend gjeografikisht te ndryshem nga biznesi I perditshem. Pjese e standartit ISO 27001.

Everest IE – Kompani Shqiptare per riciklimin e mbetjeve

EU – European Union, Bashkimi Europian

GISF - Global Institute of Sustainable Forestry, instituti qe leshon certifikata per sigurine e informacionit

GCED - Global Citizenship Education (GCED) menaxhuar nga UNESCO.

GCWN - *GCWN* do te thote GIAC (Global Information Assurance Certification) Certified Windows *Security* Administrator (software), menaxhuar nga Microsoft per sigurine e informacionit

GPPA - *GPPA*, Certified Perimeter Protection Analyst, instituti qe leshon certifikata per sigurine e informacionit

GMON – Global Monitoring Operation Network, instituti qe leshon certifikata per sigurine e informacionit

GCCC - GIAC Critical Controls Certification, certificate profesionale e sigurise qe demonstron cilesine e sistemeve IT ne respect te detyrave te sigurise.

GIAC - Global Information Assurance Certification Penetration Tester

HP – Hewlet Packard

HRM – Menaxhimi i Burimeve Njerezore

HMAC – Hash Message Authentication Code, e vlefshme per integrimin dhe authentikimin e te dhenave

IT – Information Technology

IT Security – Ekspert I sigurise se informacionit e pare ne spektrin e teknologjise

ICT - Qender Kursesh Information Communication Technology

ISO / IEC 27001 – International Standard Organization per Sigurine e Informacionit

ISO / IEC 9001 – International Standard Organization per Cilesine e Informacionit

ISACA - Information Systems Audit and Control Association

ISMS – Information Security Management Systems

ITSM – IT Service Management

ITIL - Information Technology Infrastructure Library

ILDKPKI - Inspektorati i Lartë i Deklarimit dhe Kontrollit të Pasurive dhe Konfliktit të Interesave

ISO 25001 – Standardi per menaxhim dhe planifikim

Java – Gjuhe programimi e orientuar nga objekti

MWAP - Mobile and Web Application Penetration Tester

Microsoft – Brand i sistemeve operative me popullore ne mbare boten

NAIS - National Agency for Information Society

NIS - Network and Information Security directive, udhezimet e sigurise se informacionit dhe rrjetave.

NDA – Non Disclosure Agreement, kontrata e konfidencialitetit midis nje institucioni dhe nje pale te trete.

OSCP - Offensive Security Certified Professional

Oracle - Brand i teknologjise se Informacionit

Pen Test – Procedure per te kontrolluar te gjitha breachet e sigurise ne nje institucion

QNAS - QNAP's Network Attached Storage

SQL – Structure Query Language

SIGAL – Kompania e Sigurimeve qe operon ne Shqiperi

Security + - Certifikate e sigurise se Informacionit

SoA – Statement of Applicability, qe perdoret si reference baze te standartet ISO

TCT - Qendra e Teknologjisë Tiranë

VPN-IPSec – Virtual Private Network with Information Protocol Security, komunikimi tunel midis dy pikave ne menyre te sigurte

VOIP – Voice over IP, komunikimi ne internet nepermjet zerit

TABLE OF CONTENTS

INTRODUCTION

Digital technologies have spread across critical infrastructure sectors, making it very difficult for decision-makers to understand and mitigate the risks associated with these technologies. These risks are common and global and involve national and international perspectives. Responsibility within any country is shared between the industry, which owns and operates critical infrastructure, administration and citizens.

Creating and implementing policies and tools to establish a secure communication environment is the most valuable component for managing cyber security incidents and conducting secure electronic transactions in the domestic market, in order to ensure secure electronic interaction between public authorities and citizens, businesses, enhancing the effectiveness of public and private online services, business and electronic commerce. 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 the Internet of Things (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 (NAECCS or AKCESK in its Albanian acroynum) 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 Computer Security Incident Response Team (CSIRT) is an essential component of a country's overall strategy for securing and maintaining vital technologies for national security and economic vitality. AKCESK operates in the capacity of the national CSIRT 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.

METHODOLOGY

The methodology used to complete this report includes:

1. Quantitative analysis by disseminating questionnaires to students and organizing workshops.
2. Observation and analysis of the dedicated information security profiles in all the universities of the country based on the above six pillars.
3. Conversations with the heads of public and private university departments for the first opportunity to develop information security curricula, depending on the labs and the trained pedagogical staff.
4. Discussions with the heads of IT departments of private institutions in the strategic sector (banks, hospitals) and in the manufacturing and industrial companies to observe their focus on information security in terms of:

    a. Strategic - Demand of Labor Market Demand for a 3-5 Years Strategic Period in this Sector
    b. Monetary - How much is the budget allocated by these security information institutions?
    c. Human resources - How much is the current number of people involved in the security of information in these institutions?
    d. Technical Infrastructure - How is the current security infrastructure in these institutions?
    e. Operational Problems - Has information security been impacted on day-to-day operations and how they are upgraded?
5. Recommendations on curriculum building with regard to the implementation of security techniques at the private and public universities of Albania.
6. Building the profile of information security employees based on three aspects:
    a. Security Information Implementer
    b. Information Security Analyst
    c. Information Security Auditor.

I. SUPPLY-SIDE EVALUATION: CYBERSECURITY PROFILES IN LOCAL UNIVERSITIES

We conducted an assessment of current curricula to meet the requirements of the labor market for information security employees in public and private universities. Detailed assessments are found in the Annexes.

Inventory of cybersecurity programs in public universities

Universitety	**Information Security Curriculum**
University of Tirana	1. Network Security 2. Cryptography
University of Tirana	1. Management of Secure Databases 2. Software Engineering and Security Trends 3. Cryptology 4. Advanced Information Security 5. Network Security 6. Security Planning and Incident Management 7. Information Security on Economics 8. Security of Information Systems 9. Wireless Communication Security 10. Risk Management
Polytechnic University of Tirana	1. Distributed Systems 2. Cyber Security 3. Information Security Systems
Agricultural University of Tirana	There is no information security curriculum
University "Aleksandër Xhuvani" Elbasan	There is no information security curriculum
Universitety “Fan S Noli” Korçë	There is no information security curriculum
Universitety “Aleksandër Moisiu” Durrës	There is no information security curriculum
Universitety “Ismail Qemali” Vlorë	There is no information security curriculum

Table 1 Cyber security programs in public universities

Inventory of cybersecurity programs in non-public universities

University	**CyberSecurity curriculum**
Canadian Institute of Technology	1. Network Communication and Security 2. Network Programming 3. Wireless Security 4. Web Security
Epoka Universitety	1. Security in Computer Networks 2. Information Security and Computer Analysis
Metropolitan University of Tirana	1. Computer security

Albanian University	1. Information security
Logos Universitety	There is no cyber security curriculum
Marin Barleti Universitety	1. Information and Business Management Systems
University College Luarasi	1. Network Communication and Security 2. Wireless Security dhe Web Security.
European University of Tirana	1. Risk Management in IT 2. Cryptography 3. Ethical Hacking
Professional College of Tirana	1. Information security

Table 2 Cyber security programs in non-public universities

Looking forward: universities, training centres and students

Related to future plans, a series of questions about the possibility of opening curricula for the management of Information Security were organized during discussions and meetings with pedagogical staff at private and public universities. The answers were as follows.

In the public sector:

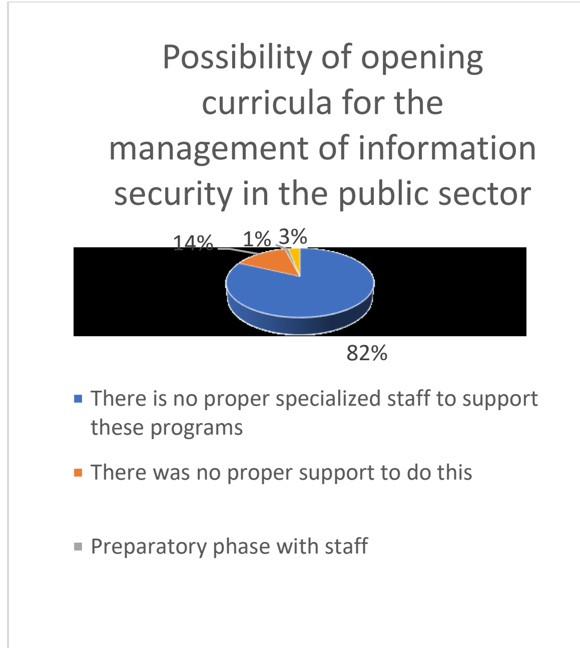

Figure 1 Curricula in public sector

In the private sector:

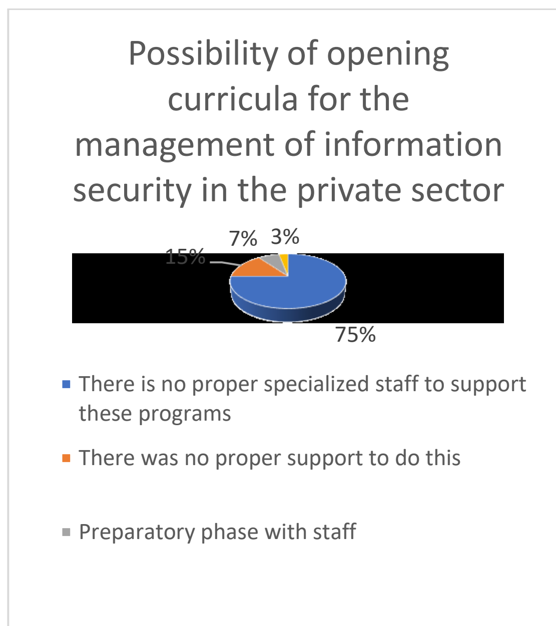

Figure 2 Curricula in non-public sector

Meanwhile, in meetings with private training providers, 100% of their responses for the question: why not to open courses for Information Security Technician and its auditors, the answer was related to the **lack of training and**

professional staff. Meanwhile, the technical side was not a problem for them.

Students' perspectives

From the answers of the questionnaire distributed to 184 students, 125 in public universities and 59 in private universities, 164 of them expressed a great interest in attending study programs in the direction of information security.

From the students surveyed, the percentage of students who expressed great interest in the field of information security is divided into: 73% professional and master of science and only 17% bachelor students.

Meanwhile, the security topics proposed in the questionnaire had a great interest to them. Some of them were:

- ✓ How can I get the wireless or router password of the neighbor's house or the nearest store - black hat 86% of the students have selected this alternative in the distributed questionnaire
- ✓ How can I protect my phone from attacks or theft of information - white hat - 86% of students had selected this alternative in the distributed questionnaire
- ✓ How can I protect the database of my web site from so-called SQL-INJECTION CODE - white hat - 86% of students had selected this alternative in the distributed questionnaire

One thing to point out was the common interest in information security fields for both genders, girls and boys. As a result of the questionnaire it was found that 53% of the students surveyed belong to boys and 47% girls.

II. ASSESSING LABOR MARKET DEMAND IN THE PUBLIC AND PRIVATE SECTOR

The purpose of this chapter is to evaluate the great potential for jobs in the field of information security in the public and private sectors of the economy.

Cybersecurity certifications

Cybersecurity 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.

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

Table 3 Certifications on cyber security

Labor demand in the public sector

In the public sector, the public institutions analyzed are:

1. Prime Minister's Office
2. Ministry of Interior

3. Line ministries and institutions in their dependence
4. National Agency of Information Society
5. Bank of Albania
6. Tirana Prosecution Office
7. Tirana Appeals Court
8. High Inspectorate of Declaration and Audit of Assets and Conflicts of Interest
9. Albanian Post
10. Alb Control

IAlmost in each of the above cases, institutions claim to implement a certain procedure without having it written. In a few cases the institutions delegate their responsibility to the NAIS, such as e-mail access procedures, information security policies, etc.

From the above data, we can conclude in the following two graphs, to see the ratio of IT worker to security employees in each sector, as follows:

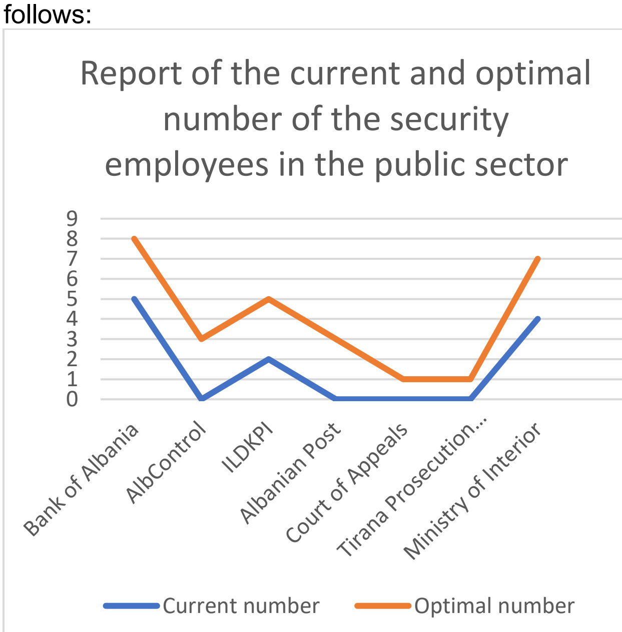

Figure 3 Report of the current and optimal number of security employees in the public sector

The graph shows the lack of staff of security experts. According to the best European practices and domestic legal framework for the security team in critical and important information infrastructures, the following graph shows the current number and optimum number of public sector security employees.

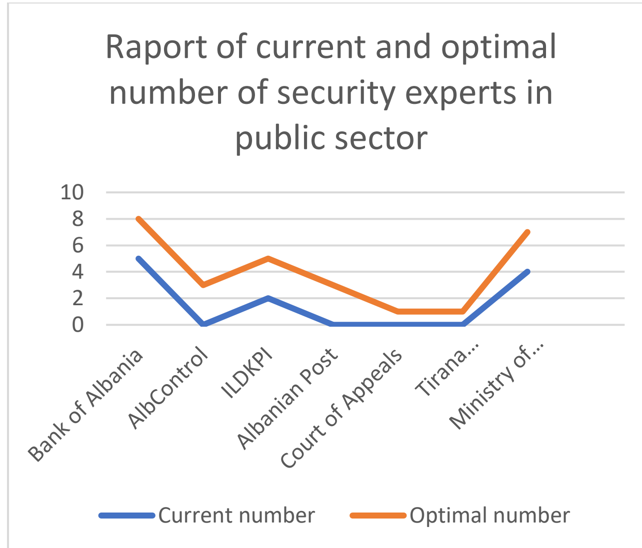

Figure 4 Report of the current and optimal number of the security employees in the public sector

Employee perspectives

Based on the analysis and conversations conducted with private and public sector employees, it was found that:

Public sector:

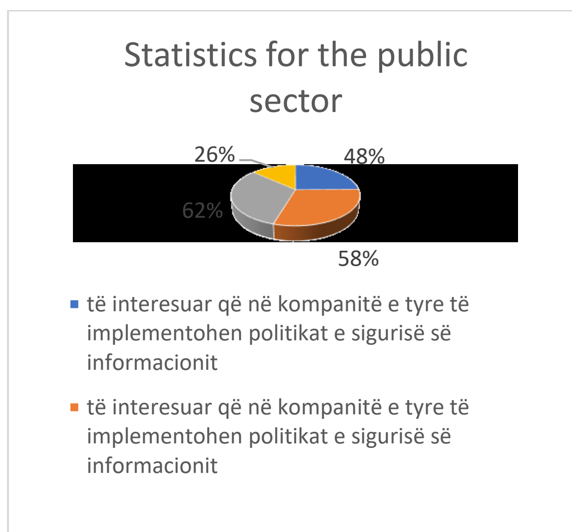

Figure 5 Statistics for public sector

a. 48% of employees of public institutions are interested in implementing their information security policies in their companies
b. 58% of managers of public institutions are interested in implementing their information security policies in their companies
c. 62% of employees in the IT department of public institutions are interested in studying and training in the field of cyber security
d. 26% of employees in the IT department of public institutions are interested in studying and training in the field of information security auditing

Private sector:

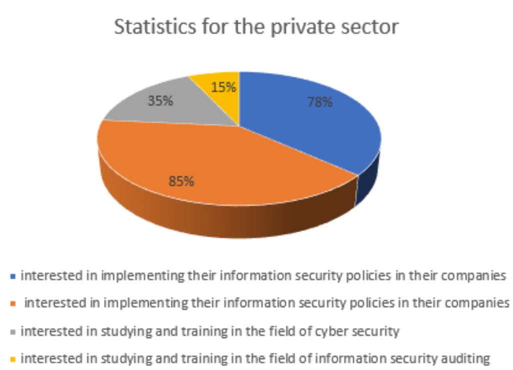

Figure 6 Statistics for private sector

- 78% of employees of are interested in implementing their information security policies in their companies
- 85% of managers are interested in implementing their information security policies in their companies
- 35% of employees in the IT department are interested in studying and training in the field of cyber security
- 15% of employees in the IT department are interested in studying and training in the field of information security auditing

<u>Demand and supply of IT security employees in the labour market</u>

To study this report, it was analyzed the trend of the level of employment of students who have followed and completed their studies according to the categories below:

a. Academic education in the field of information security (Faculty of Information Economics, Cybersecurity course)
b. Courses in the direction of technical security and auditing (Cisco Security, Linux Security, Windows Security, Web Security, Network Security, Penetration Testing, Ethical Hacking, Mobile Security, ISACA, COMPTIA, ISO etc.)
c. Academic education in the field of information security abroad

For the three above categories after ad-hoc meetings with representatives of the IT department and security in the public and private sector, the data collected are represented in the following tables. The analysis is done only for two directions:

Technical security										
Private institutions										
	Banks		**Insurance compani**		**Manifacture compani**		**Telephone compani**		**Hospitals**	
Year	*Demand*	*Employm*	*Demand*	*Employm*	*Demand*	*Employm*	*Demand*	*Employm*	*Demand*	*Employm*
2016	110	15	20	15	10	10	70	20	15	15
2017	115	20	20	15	10	10	75	20	15	15
2018	125	15	25	20	10	20	80	25	20	25

Table 4 Technical security demand-supply report in private sector

Technical security						
Public institutions						
	Government		**sh.a institutions**		**Juridical system**	
Year	*Demand*	*Employment %*	*Demand*	*Employment %*	*Demand*	*Employment %*
2016	80	20	35	15	10	10
2017	85	20	35	20	10	10
2018	90	25	40	20	15	15

Table 5 Technical security demand-supply report in public sector

Security audit										
Private institutions										
	Banks		**Insurance compani**		**Manifacture compani**		**Telephone compani**		**Hospitals**	
Year	*Demand*	*Employm*	*Demand*	*Employm*	*Demand*	*Employm*	*Demand*	*Employm*	*Demand*	*Employm*
2016	70	20	10	10	5	20	20	10	10	10
2017	75	20	10	15	7	20	25	15	10	10
2018	85	20	10	20	8	20	25	20	10	10

Table 6 Security audit demand-supply report in private sector

Security audit						
Public institutions						
	Government		**institutions**		**Juridical system**	
Year	*Demand*	*Employment %*	*Demand*	*Employment %*	*Demand*	*Employment %*
2016	40	10	15	15	5	20
2017	50	20	15	20	5	20
2018	50	25	15	20	5	30

Table 7 Security audit demand-supply report in public sector

Evidenced differences in filling vacancies in the labor market are a consequence of failure to meet a number factors as follows:

1. Measurement the investment of creating a job IT security in two aspects:
    a. Managing of Human Resources / Education and training.
    b. IT Support, consist of Hardware / Software /Communication a. Menaxhimi i Burimeve Njerëzore / Arsimi dhe trajnimi.

2. The number of employees in the security department depending on the size and profile of the company

3. Assessment of security investment to outsource IT Security services to third parties

Investments in Human Resources for Information Security are classified into:

1. 1. Hiring a **CISO** in a company. This is a person responsible for implementation of all policies and procedures of security standards in company in high level, encourage line managers in implementation of ethical decision making process. At the same time, he is the authoritative person for communication and reporting to Board members, shareholders and sponsors related to security concerns in company.
2. CISO must be educated in Information Technology or related disciplines.
3. CISO must have a wide experience (more than 5 years) in implementation of security issues.
4. CISO must be certified by ISO 27001 standard. This certificate must be refurbished periodically.
5. Would be preferable if he is certified in CompTIA Security+, CISA, CISM, Pen Test etc.
6. Hiring a **Forensic Analyzer Senior** for analyzing, monitoring and penetration network, database or software specialist.
7. His/her scope is in scanning network ports, gathering the evidences of web vulnerabilities, checking the database vulnerabilities, analyze the vulnerabilities, assess the database management system performance, checking the weakness in password attacks, controlling the flaws of wireless attacks, doing the reverse engineering procedures, using the exploitation tools, managing and revealing the sniffing and spoofing techniques, finding generic tools of security managing and social engineering.
8. Forensic analyzer senior must have experience in network and systems security. Is preferable to be equipped by some certification such as: CISP, CEH, CISA, A+, CASP+, CCSP, CCNA, CISM, Network+, CERT-CSIH, CGEIT, CRISC, Security+, Ethical Hacking or Pen testing. Education of Forensic analyzer should be in the alignment of Information Technology scope
9. Hiring a **Forensic Analyzer Specialist** for supporting the activities of network/system security monitoring and analyzing. His/her education should be in the alignment of Information technology scope. Certification in security profile would be welcome too.
10. Hiring an **Auditor Senior** for implementation the policies and procedures in low level, inside the unit of a company. He/she will take care of employee`s training in security policies and procedures inside the company. He/she will be participating actively in data analyzing and ISO implementation with IT Steering committee and frequently should deliver reports to CISO
11. His/her education should be in the alignment with Information Technology scope. He/she must be certified in some of the following certifications: ISO 27001, ISO 9001, ISO 25001, COBIT, CISA, CISM and CISP (or equivalent).
12. Hiring an **Auditor Specialist** for supporting of daily activities auditor senior. His/her education should be in the alignment with IT scope and it would be preferable to be certified in at least one of the following certificates, such as: CISA, ISO 27001, Network+.

III. PREVIEW OF INVESTMENTS FOR ESTABLISHING A SYSTEM (HARDWARE, SOFTWARE, HUMAN RESOURCES) OF A HIGH SECURITY LEVEL

Establish the system / infrastructure (hardware, software and communication line) insource

a. Determine the procedural steps and functionality of the system / infrastructure according to the order below:

- o Obtain Management support and approval
- o Identify and understand requirements and expectations of interested parties
- o Document the ISMS scope based on the Group agreed scope statement as specified below:
- o Supplier Management
- o Third Party Service Level Management
- o Service Catalogue Management
- o Availability Management
- o Configuration Management
- o Service Testing and Validation
- o Release and Deployment Management
- o Change Management
- o Event Management
- o Incident Management
- o Asset Management and Monitoring
- o Network Management and Monitoring
- o Service Management and Monitoring
- o Event Driven Process Management

- Document the Information Security Policy

- Document roles and responsibilities as part of the Information Security Policy and Supporting Policies
- Define the information security risk assessment process
- Apply the information security risk assessment process
- Select control objectives and controls for risk treatment
- Prepare and publish the Statement of Applicability (SoA)
- Drafting of Specific Security policies & procedures
- Develop the formal Risk Treatment Plan
- Monitor & review
- Monitor & improve
- Risk Identification, Management and Analyzing

b. Cost of Investment per year of Human Resource / Insource

Profile	Salary / Year (Gross)
CISO	25 000 – 50 000 Euro
Forensic Analyzer Senior	20 000 – 35 000 Euro
Forensic Analyzer Specialist	15 000 – 20 000 Euro
Auditor Senior	20 000 – 25 000 Euro
Auditor Specialist	10 000 – 15 000 Euro
TOTAL	90 000 – 145 000 Euro

Table 8 Annual costs on the profile of employees

a. Estimating costs for implementing standards for a high level of security

Each company should support the technology implemented in a system / infrastructure in implementing standards to reach a high level of security. The number and type of hardware, software and basic infrastructure depends on various factors such as: Company size, Distance between company and branches, Company profile, revenues, scope of security etc. However, the following table describes the type of equipment associated with the software and the necessary communication infrastructure to successfully implement the IT Security strategy in an average company.

Devices	Business Process	Cost
Servers 2-8	Monitoring the traffic, analyze the vulnerabilities, store logs, store the documents, management of backup process, keep the record of security incidents and increase the level of authorization	1 500 – 5 600 Euro
Network Infrastructure 2 per peer	Implementation of VPN tunnels among branches and HQ of the company (no. of branches depend of the company size)	200 Euro -> Implementation work
Quality Services in security form by VOIP	Build up the Call Manager VOIP Telephony by using CIA approach	2 000 – 20 000 Euro
Routers and Switches 2 – 4 Routers 2-8 Manageable Switches Depends of company infrastructure	Storing/forwarding and switching the packets in security mode	10 000 – 15 000 Euro
Firewall 1	Inspect the traffic	1 500 – 3 000 Euro
Software for: Monitoring the state of company and generate a report based on ISO 27001 Standard	Monitors and notifies if a breach has occur	Free (Open Source Tools) up to: 3 000 Euro (Business Tools)

Software for: Check the traffic of the services implemented by company	Monitor for traffic vulnerabilities, system vulnerabilities, web vulnerabilities, network vulnerabilities and patch it automatically	Free (Open Source Tools) up to: 1 000 Euro (Business Tools)
Software for: Verify the critical services toward the customers and other partners (B2C and B2B)	Check the integrity and authentication data toward the customers or partners	Free (Open Source Tools) up to: 200 Euro (Business Tools)
Software for: log reporting and generation	Generate automatically a daily/weekly/monthly report and inform any suspicious action has occurs.	Free (Open Source Tools) up to: 500 – 1 000 Euro
Software for: Network Configuration alerts	If the network is configuring improperly, it informs automatically to the owner or network administrator.	Free (Open Source Tools) up to: 500 – 1 000 Euro
Maintenance	Maintenance process per year/depends of company size and profile	Free – 10 000 Euro
TOTAL		**15 200 Euro – 60 000 Euro**

Table 9 Costs for creating an IT security job insource

b. Human resource needs by range and profile of a company

Nr of Employees	Company Size	Profile
8 – 15	50 – 500	Bank
5 – 10	20 – 100	Insurance Company
5 – 10	10 – 200	Services Company
8 – 20	40 - 1200	Telecommunication company
3 – 6	20 – 200	Manufacture
4 – 8	40 – 800	Hospitals
2 – 5	30 – 300	Education (pre-university)
3 – 7	40 - 400	University

Table 10 Human resource needs by range and profile of a company

Estimation of costs in case of transfer the services on the security functionality of systems / infrastructure to the third parties (outsource)

Business Process	Nr of specialists (outsource part)	Scope of company	Retention time	Accountability (insource part)
Monitoring the state of company and generate a report based on ISO 27001 Standard	2 Security Specialist + CISO	All departments	3 months –5 months (Depends from company size and scope of standard implementation)	HRM + Legal + IT Manager
Check the traffic of the services implemented by company	1 Security Specialist	IT Department	1 month	IT Manager

Verify the critical services toward the customers and other partners (B2C and B2B)	1 Security Specialist + CISO	IT Department	1 week	IT Manager
Implementation of ISO Security standard	2 Security Specialist + CISO	All departments	6 months – 15 months (Depends from company size and scope of standard implementation)	HRM + Legal + IT Manager
Training of employees based on ISO Standard	1 Security Specialist	All departments	2 months (Depends from company size)	HRM Department
Documentation of ISO standard	CISO + 1 Security specialist	All department	3 months – 5 months	IT Manager
Internal audit implementation	CISO	All department	2 months	IT Manager + HRM Department
White Hat penetration – catch the flag techniques over: Vulnerabilities in web, database, password policies , wireless, communication , mail, firewall and dns.	2 Security Specialist	IT Department	1-2 months (Depends from the number of services)	IT Manager
Analyzing and patching the problems rise up by pen-testing technique	2 Security Specialist	IT Department	1-2 months (Depends from the number of services)	IT Manager
Check the contract with third party and amendment of NDA	CISO	All Department	1 month	HRM Department
Post-Monitoring	CISO + 2 Security specialists	IT Department	12 months	IT Manager

Table 11 Estimation of costs in case of transfer the services on the security functionality of systems / infrastructure to the third parties

Cost of implementation of ISMS, started out (depends of the company size and the status of implementation) **5 000 Euro - 25 000** Euro per year. Companies with more than 200 employees and with large scope of auditing it can be reach up to **50 000** Euro per year

Cost of White Hat (Technical security implementation) certainly varies in accordance to company size and scope that companies has been agree upon their requests. Anyway, it can have started out to **5 000 Euro** and end up to **20 000 Euro**. Cmpanies with more than 200 employees and with a large scope of security implementatio can reach up to **50 000 Euro** or more per year.

In Albania, there are 4 companies which operate in implementation and management of security standards as outsourcing toward the Albania business. Three of them operate as consulting of ISO security standards and only one company operate as “white hat” and tries to find breaches and flaws in business activities.

It`s scope covers as the following:

- Gathering the information
- Analysis the vulnerability
- Web application vulnerabilities
- Database injection malicious code
- Password attacking
- Wireless vulnerabilities analyses
- Post exploitation, sniffing and spoofing implementation
- Reverse engineering and system services implementation.

95% of Albanian market has cover by these 4 companies and only 5% managed by foreign companies. I want to stress out that these companies (5 % of Albanian companies) operate as a branch of their HQ located at Europe such as: banks, mobile companies, insurance etc. These companies cover roughly 80% of security implementation insource and only 20% managed by the external services and employees.

IV RECOMMENDATIONS FOR IMPROVING THE CURRENT SITUATION IN THE FIELD OF CYBER SECURITY

IV.1 Recommendations for Universities

a. Enrichment of curricula in private and public universities in the field of information security, which should be implemented only in cycles:
   - Professional Master with 60 credits - 1 year
   - Scientific Master with 120 credits - 2 years

b. Implementation of information security should only be done in the professional and scientific masters and not in bachelor's degree for two reasons:
   - Information security needs to be developed after a good theoretical background in several other preliminary areas such as: Computer Networks, Operating Systems, Computer Architecture, Programming Languages, Web Developments etc.
   - A good practical foundation and preliminary laboratory experience is required before the White Hat safety techniques are implemented.

c. The curriculum in these institutions will be based on three areas:
   - Information Security Techniques
   - Security Data Analysis
   - Data security audit

d. Regarding the point of information security techniques, the following issues should be implemented in university curricula:

- Patch problems and control for their improvement
- Finding network problems and related operations
- Penetration on the policy security system and access lists
- Penetration on the data security system and elimination of malicious injection
- Penetration over what is called the black box - Catch the flag
- Pentagram on Web Techniques
- Digital investigation analysis
- Security Systems
- Traffic monitoring and packet inspection systems

- Systems of vulnerability and follow-up
- Building a secure network infrastructure
- Defining the policies and objectives of the security of the respective institution
- Assign roles and responsibilities
- User rights, applications, and password usage
- Defining security incidents
- Defining mobile device policies
- Determining security operations
- Determining the Business Continuity Plan and Mass Destruction (BCP and DRP)

IV.2 Recommendations for private training centers

a. Establishment of good student training centers that are being formed through current curricula in ICT branches in all universities and orientation of existing ones, towards the implementation of information security issues, in meeting market requirements by categorization in the above fields in profiles:

- Microsoft Security +
- Linux Security +
- CCNA/CCNP Security
- Comptia Security +
- Digital Forensic
- Penetration Testing
- Certified Ethical Hacker - CEH
- ISO 27001
- CISM – Certified Information Security Manager
- CISA - Certified Information System Auditor
- CISP – Certified Information System Security Professional
- GIAC Security Essentials
- Cyber Defense
- GIAC Certified Intrusion Analyst
- GISF
- GCED
- GCWN
- GPPA
- GMON
- GCCC
- CRISK

Courses are required to be intensively pursued, over a period of 3 to 4 months, to absorb the basic information needed to qualify them according to market requirement.

IV.3 Recommendations for public and private sector operators to provide and enhance security levels in information systems / infrastructures

a. To ensure the implementation of security procedures and to fulfill the role of CSIRT, the employees of the institutions (responsible group) should be trained on how to react and deal with potential cyber incidents.
b. 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.
c. 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.
d. 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.

e. 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.

V. WORK PROFILE FOR INFORMATION SECURITY EXPERTS

In order to implement adequate security levels, three categories of employees are needed:

a. Information security technician
b. Information Security Analyst
c. Information security auditor

A private company with critical and important infrastructures to meet the requirements of the cyber security law and its by-laws to ensure a high level of security should employ all three of these profiles as a part of CSIRT- sectoral.

V.1 Information security technician

Responsibilities and duties of the Information Security Specialist

- Insure information system assets by identifying and solving potential and current security problems.
- Performs simulated attacks on network, firewalls, operating systems, and web applications are at the center of work.
- Identify weaknesses and report on findings.
- Faces internal and external clients
- Protects the system by setting access privileges, control structures, and resources.
- Recognize problems by identifying anomalies; reports security breaches.
- Implement security improvements by assessing the current situation; trend estimation; anticipating the requirements.
- Determines security breaches and inefficiency by performing periodic audits.
- Improve the system by implementing and maintaining security controls.
- Informs the user by preparing performance reports; communicating the status of the system.
- Maintains quality service by following the standards of the organization.
- Maintain technical knowledge by following workshops.
- Contributes to team efforts by performing similar results as needed.
- Selects, designs and creates suitable tools for testing
- Perform penetration testing on computer systems, networks, applications on the Internet and / or mobile
- Documents the working methodology

V.2 Information Security Analyst

Cyber Security Analysts help protect an organization by using a variety of technologies and processes to prevent, detect and manage cyber threats. This may include the protection of computers, data, networks, and software.

Information security analysis can be divided into two subclauses:

• Counseling, providing consulting services to clients

• protecting the security of the organization you work for.

Job titles vary and may include information security analysts, security analysts, information security consultants, the Security Operations Center (SOC) analyst and cyber intelligence analyst.

Responsibilities and Tasks of Cyber Security Analyst:

• Be up-to-date with the latest security and technology developments

• Investigate / evaluate increased threats to cyber security and ways to manage them

• Draft a disaster recovery plan in case of any breach of security

• To monitor systems for unusual, unauthorized or illegal attacks, interference and activities

• Test and evaluate security products

• Use advanced analytical tools to determine patterns of emerging threats as well as their weaknesses

• Use "ethical piracy", for example, by simulating security breaches

• Identify possible vulnerabilities and enforce security measures, such as firewalls and encryption

• Investigate security notifications and ensure incident response

• Monitor misuse of permits by authorized system users

• Interconnect with stakeholders on cyber security issues and provide future recommendations

• Generate reports for technical and non technical staff, as well as stakeholders

• Maintain a register of information security risks and assist with internal and external audits related to information security

• Monitor and respond to phishing email and pharming activity

• Help create, maintain and disseminate cyber security awareness training for peers

• Provide staffing advice and guidance on issues such as spam or unwanted or malicious e-mails.

V.3. Auditor in Information Security

The Information Security Specialist (ISO) is responsible for providing appropriate security controls for information assets. ISO protects information by seeing that security risks are identified, evaluated and reported accurately. In addition, the ISO is tasked with providing local procedures and activities in accordance with all regulatory requirements and internal policies, procedures, guidelines and standards. ISO is the center of competence for information security that provides a role of advisory services and acts as a focal point for activities and responsibilities related to security compliance.

Auditor's Responsibilities and Tasks in Information Security:

- Maintain the Department of Information Security and policies, procedures, standards and guidelines
- Takes the lead in developing, maintaining and updating the Information Security Strategy and Information Security Program
- Provides actively the appropriate administrative, physical and technical measures to protect the information assets from internal and external threats
- Identifies, implements and enforces appropriate procedures, including controls and balances, to regularly test these safeguards
- Completes annual reviews and audits as needed by engaging internal business partners throughout the organization and external resources
- Sets a priority to see that disaster recovery and emergency operation procedures are set and tested on a regular basis
- Acts as a committed owner of security incident and vulnerability management processes from design to implementation and beyond
- Manages and assists in carrying out continuous monitoring of information systems security, including risk assessment of information security through quality risk analysis on a regular basis, performing functional analysis and gap to determine the extent to which key business areas and infrastructure comply with the statute and regulatory requirements, assess and recommends new information security technologies and countermeasures against threats to information or privacy, as well as

development of security reports and control panels

- Provides effective staff training programs to raise awareness of security. Maintaining and encouraging open business relationships within the team
- Is a model for organizational culture, creating a positive impact in every contact with people
- Ensures active participation in community events as part of the overall commitment to Corporate Social Responsibility
- Improves the work processes to realize the cost and resource efficiency
- Considers health and safety as a primary concern to ensure the overall well-being of his team and other members

Required skills

- Possess CISSP, CISSLP, GIAC or other security certifications at similar levels
- Possesses negotiating skills
- Demonstrates knowledge about the risk of information security and best industrial practices
- Fast response to customer requests
- Is flexible and adapted to change
- Share knowledge with others
- Shows a high level of integrity and is trustworthy
- Possesses excellent communication skills
- Use the courage to take action in harsh situations
- Does the right things for the right reasons.

ANNEX 1: ANALYSIS OF CYBERSECURITY CURRICULA IN PUBLIC UNIVERSITIES

In the first university analyzed **are registered for the academic year 2018-2019, 166 new students, of whom 94 students are boys. The total number of students enrolled in bachelor education is 420, out of which 266 are boys, while in the master course there are 183 students, out of which 111 are boys.** In these three departments there are 46 internal lecturers, but only four of them have a solid background in the field of information security.

Forty-two (42) pedagogues of these departments are pedagogues with titles. This university has three study cources:

1. Bachelor
2. Professional Master
3. Master of Science

2 years ago (2016) was an attempt to open the direction of Information Security but did not succeed due to the low number of specialized pedagogues in this field.

In these three directions, there are few subjects focusing on the Information Security field.

In the bachelor cource: Distributed Systems and Cyber Security - In Computer Engineering

In the Master of Science cource: Information Security Systems - In Information Engineering

In the branch of Telecommunication Engineering and Electronics, the bachelor cource has no subjects related to the field of information security, but there are only a few topics within the "Computer Networks" module.

Meanwhile, in this Master of Science course is the module: Network Security, which deals with cyber security issues in networks.

This faculty has been accredited for three years by the British system. However, there is a considerable lack of laboratory infrastructure. Computers are not connected to the network and there is no continuous internet, which makes it impossible to develop normal information security modules.

The security field in this faculty covers about 10% of the total topics contained in the syllabus of the three departments.

At the second faculty analyzed are enrolled for the academic year 2018-2019, 174 new students, **of whom 77 are boys. In total there are 535 students enrolled in bachelor education, out of which 245 are boys. Meanwhile, there are 236 students enrolled in the master and scientific master course, out of which 106 are boys.** There are 17 internal pedagogues in this department, but none of them have a proper background in the field of information security.

14 pedagogues of these departments are pedagogues with titles. This university has three courses:

1. Bachelor
2. Professional Master
3. Master of Science

In this department, in the bachelor course is conducted: the Cryptography module, which has more mathematical connotation than that of information security.

In the Professional Master and Master of Science courses is developed: the "Safety in Network" module which, apart from some theoretical concepts, has a significant lack of practical sense. Meanwhile, other topics do not address issues related to information security.

This faculty has been accredited for three years by the British system. However, there is a considerable lack of laboratory infrastructure. Computers are connected to the network, but it does not have regular maintenance and does not have constant access to the Internet, which makes it impossible for the normal development of information security modules.

Also, in this university, despite the fact that there is a very high number of professors with title, their background is irrelevant to the field of information security.

Topics dealing with information security concepts cover about 20% of the total topics covered by the professors of this department.

At the third university analyzed, the respective deparment is composed of bachelor and master courses in Business Informatics, and has a number of 25 lecturers, of whom 21 possess titles.

In the bachelor course, there is no tendency in the field of information security, but this department has opened a cyber security program in cooperation with a university in Norway, in the Master of Science course, **where participate 67 students, of whom 28 are boys.** The subjects are as follows:

a. Management of Secure Databases
b. Software Engineering and Security Trends
c. Cryptology
d. Advanced Information Security
e. Network Security
f. Security Planning and Incident Management
g. Information Security on Economics
h. Security of Information Systems
i. Wireless Communication Security
j. Risk Management

From the above, the last two courses are in student's choice.

What has been observed from the syllabus is that:

Management of Secure Databases is more focused on databases than on their security

Software Engineering and Security Trends - In this subject is completely developed the subject of Software Engineering, and there are no issues related to their safety

Cryptology – Issues similar to the Cryptography subject are treated.

Advanced Information Security – In this subject are treated Computer Network Trends and their Security. Parts of this subject are elements of cyber attacks, firewall policies, and some concepts of viruses and worms.

Network Security - This topic addresses issues related to computer networks, and some concepts of Firewall, Port Security in the second layer of OSI Architecture and Tunnels.

Security Planning and Incident Management - This subject is related to the information security audit system and specifically based on the ISO 27001 model. The curriculum is rich in concepts and offers students the opportunity to integrate into the labor market.

Information Security on Economics - The subject addresses economic concepts related to security and information security.

Security of Information Systems - The subject addresses issues related to viruses, worms and ISO standards.

Risk Management - Handles information security risk and management issues.

Wireless Communication Security - The course syllabus is rich with a tutorial that helps students practice theoretical concepts. This course is optional.

In the internal staff only two pedagogues have the proper background in information security. The department has cooperation with a Norwegian university, enabling pedagogues to exchange experience on certain modules with the students of this department.

In order to train students, two laboratory halls with 25 and 35 computers in the network dedicated to information security have been constructed. This opportunity serves the students of this department to learn security issues not only from a theoretical concept, but also from a practical point of view

In the bachelor course, topics related to information security are not addressed.

On the other hand, the topics developed in the Master of Science and professional master, excluding the CyberSecurity branch, cover only 5% of the security field. Meanwhile, the CyberSecurity branch covers 100% security issues.

In the fourth faculty, are enrolled for the academic year 2018-2019, **64 new students, of whom 36 are boys. In total, there are 176 students enrolled in this bachelor's program, out of which 94 are boys. Meanwhile, there are 32 students enrolled in the Master of Science degree, out of which 25 are boys. There are 16 students enrolled in professional master courses, out of which 12 are boys.** There are 15 internal pedagogues in this department, but none of them have a proper background in the field of information security.

What is noticed in this department is the lack of professional laboratories. There are two halls that cannot cover the required capacity.

Laboratories have a computer network where PCs are connected, but their lack of maintenance and the lack of internet access do not provide the right conditions for students.

13 pedagogues of these departmentsposses' titles. This university has three courses:

1. Bachelor
2. Professional Master
3. Master of Science

In the bachelor courses there are no subjects directly related to the cyber security field.

The same can be said about the master courses in this department. Meanwhile, in the Master courses is a module in the field of Information Security, named Information Security Systems and Security Networks. Other subjects do not contain topics related to the field of information security.

The security field covers only 5% of topics in this department.

In this next university analyzed, are registered for the academic year 2018-2019, **143 new students, of whom 79 are boys. Meanwhile in the bachelor courses are registered 236 students, of whom 130 are boys, and in the professional and Master of Science courses, as well as the two-year college, are registered 224 students, where 116 are boys.** There are 36 internal pedagogues in this department, but none of them have a solid background in the field of information security.

What is noticed in this department is the lack of professional labs. There are three labs that can not cover the required capacity for students.

Laboratories have a computer network where PCs are connected but the lack of maintenance and the lack of internet make this system unable to cope with the relevant work of students.

28 pedagogues of these departmentsposses titles. This university has three courses:

1. Bachelor
2. Professional Master
3. Master of Science

In the bachelor course there are no subjects directly related to the cyber security field. The same can be said about the master courses in this department.

The security field covers only 7% of topics in this department.

In the sixth university, are enrolled for the academic year 2018-2019, **58 new students, of whom 34 are boys. Meanwhile, there are 98 students enrolled in the bachelor course, out of which 56 are boys. There are about 54 students enrolled in professional and Master of Science courses, with 33 being boys.** There are 31 students enrolled in the 2-year college, where 21 are boys. There are 7 internal pedagogues in this department, where only one of them has a solid background in information security, who has studied abroad.

What is noticed in this department is the lack of professional labs. There are two labs that can not cover the required capacity for students.

Laboratories have a computer network where PCs are connected, have ongoing maintenance and internet but lack the specific infrastructure to provide the practical side of information security issues.

5 pedagogues of these departments are pedagogues with titles. This university has three courses:

1. Bachelor

2. Professional Master
3. Master of Science

In the bachelor course there are no subjects directly related to the cyber security field.

Meanwhile, for the professional and Master of Sciences courses in this department, the Information and Network Security module is developed, which theoretically covers the security issues in this discipline. **However, the security field covers only 12% of topics in this department**.

In the other university, for the academic year 2018-2019, are enrolled 44 new students, of whom 29 are boys. There are 111 students enrolled in bachelor course, out of which 61 are boys), while in the master course are registered 42 students, of whom 26 are boys. In the 2-year college there are 17 students enrolled, of whom 11 are boys. There are 11 internal pedagogues in this department, but none of them have a solid background in the field of information security.

What is noticed in this department is the lack of professional labs. There are two labs that can not cover the required capacity of the students.

Laboratories have a computer network where PCs are connected, have ongoing maintenance and internet but lack the specific infrastructure to provide the practical side of information security issues.

5 pedagogues of these departments possess titles. This university has two modules:

1. Bachelor
2. Professional Master

In the bachelor cycle there are no subjects directly related to the cyber security field.

Meanwhile, for the professional master cycle in this department, the Information Security module is developed, which theoretically covers the security issues in this discipline. **However, in total, the information security covers only 5% of the total topics in this department**.

In the last university, for the academic year 2018-2019, **36 new students, of whom 25 are boys. The number of students in the bachelor course is 96 out of which 56 are boys. Meanwhile, there are 34 students enrolled in the Masters courses, of whom 27 are boys.** There are 7 internal pedagogues in this department, but none of them have a solid background in the field of information security.

What is noticed in this department is the lack of professional labs. There are two labs that cannot cover the required capacity of the students.

Laboratories have a computer network where PCs are connected, have ongoing maintenance and internet but lack the specific infrastructure to provide the practical side of information security issues.

5 pedagogues of these departments possess titles. This university has two courses:

1. Bachelor
2. Professional Master

In the bachelor course there are no subjects directly related to the cyber security field.

Meanwhile, for the professional master course in this department, the Networks Security module is developed, which theoretically covers the security problems in this discipline. **Information security covers only 7% of the total topics in this department.**

As per above, summarized, the chart below shows the number of students in public universities in the country, categorized by gender and study course.

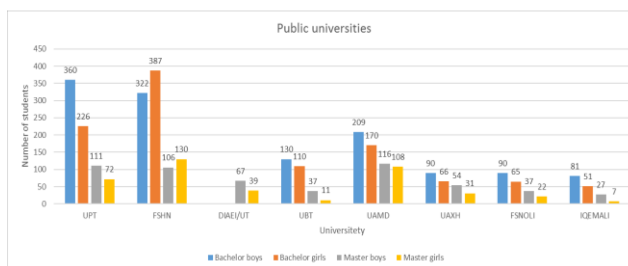

Figure 7 Students in the public universities

The graph shows that the highest number of boys is reached in the Bachelor program is the Polytechnic University of Tirana, the highest number of girls in the Bachelor program is reached in the Faculty of Natural Sciences, the highest number of boys in the master cycle is the

University Polytechnic University of Tirana and the highest number of girls in the master cycle is reached at the Faculty of Natural Sciences.

ANNEX 2: ANALYSIS OF CYBERSECURITY CURRICULA IN PRIVATE UNIVERSITIES

In the first university analyzed, in the bachelor and master level program is the first year that the Information Technology direction is developed, and the number of students enrolled at the bachelor level in this branch is 30 students, of whom 21 are boys and 9 girls and in the master level, the number of registered students is only 12 students, out of which 9 are boys and 3 girls. Similarly, students are enrolled in the Professional Master program, of which 10 are boys and only 2 are girls in the Cyber Security Management. These figures are significant considering the short time of starting these study branches. There is no Master of Science level in the field of Cyber Security in this university.

The number of 12 students in the professional master in the field of cyber security, which is in the first year at this university, is a very good signal that shows the interest to have young people in this field.

It can be consired as the courage and initiative of the board of this university, to open a branch in the field of information security as a response to market demands.

From the observations of the laboratories of this university is found out that two laboratories have 24 desktop computers with internal network and internet, as well as the lack of other professional equipment needed to increase the efficiency of the work and the professionalism of the students. There is no RACK device with at least 2 routers and 2 switches, and there is not at least one server where students can work in order to complete their course assignments.

Despite the fact that the cyber security management in a master program is part of the curriculum of this university, only a few subject are related with the implementation and developing of students' knowledge in information security. Subject related to information security are: Network Communication and Security, Wireless Security and Web Security. Often for these modules, subject programs do not fully comply with the field of information security, and references need to be updated.

From the analysis of the pedagogical staff assigned to teach at this university, two elements have been identified:

- Lack of pedagogical staff to cover information security issues and attracting experts of the field
- Lack of competence of pedagogues in relation to information security branches

Students, in order to successfully complete tasks and projects in the field of information security utilize a simulator instead of a real environment.

In the second university analyzed, in the bachelor and master's level program were defined specialized directions in the field of information systems.

In the bachelor's level for the current year, **there are 54 students, out of which 33 are boys and 19 girls**, in Software Engineering, IT and Telecommunication. All three of these profiles are accredited for a period of five years by the British system.

Meanwhile, there are currently 34 students enrolled in the MSc in Engineering, IT, Big Data, Web Developments, Cyber Security and Telecommunication, **of whom 21 are boys and 13 girls**. In addition to the Big Data and Cyber Security Directions, which have their second year since their opening, the other three directions are accredited for a period of five years by the British system.

So, in the master courses, this university has opened up the course of Cyber Security. It is worth mentioning that the number of enrolled students in this **regard is 11 students in the first year and 12 students in the second year, where in both cases the number of boys is 8 students.**

Despite the fact that cyber security management in the master's level program is part of the curriculum of this university, few have to do with the implementation and deepening of students' knowledge in information security. Subjects related to information security are: Network Communication and Security, Network Programming, Wireless Security and Web Security. It has been noticed that even for these modules, course programs do not fully comply with the field of information security as well as references need to be updated. The practical part of the lab is covered with some simulators such as Cisco Packet Tracer.

From the analysis of the pedagogical staff assigned to teach at this university, two elements have been identified:

- Lack of pedagogical staff to cover information security issues
- Lack of competence of pedagogues in relation to information security branches

In the third university was only one branch in the bachelor level related to computer science: Electronic Engineering. Meanwhile, in the Master of Science level there is also only one branch, Electronic Engineering. In this university there are only a few subjects dedicated to information security. There are only two subjects in MSc in Electronic Engineering:

a. Security in Computer Networking

b. Information Security and Computer Analysis

The theoretical part is treated very well and the references are relatively new, but what is noticed here is the total absence of laboratory classes. Network security only comes with a simulator and can only cover some topics that concern port security in OSI's second layer, IPSEC VPN policies, and some simple implementations using Cisco Firewall Access Lists. What we can also mention here is that in the lab is treated only one kind of technology of information security, CISCO.

The number of students enrolled this year at the branch of Electronic Engineering in bachelor courses is 64 students, of which 35 are boys, and in master level the number of students is 42, of which 22 are boys. What is noticeable at this university is the average student level coming from secondary schools, which is higher than those from other private universities. Accreditation of Computer Engineering and Business Informatics courses has been done for 5 years by the British system.

In the fourth university were two branches oriented to information systems in the Computer Engineering, and Business Informatics branches and has only one subject in the field of Information Security, which is developed in the Master of Science in the second year and is called Computer Security. So it is just a single subject to cover all the information security capacity of students. This course has 60 hours of which only 15 hours are laboratories classes. In this university students have PCs but Internet problems and computer settings make it impossible to implement security information at these laboratories.

The pedagogical staff assigned to the master courses is over-aged, about 40% of them are retired, which makes it doubtful for the implementation of the security field towards the students because this field is very young in Albania. Accreditation of Computer and Economic Informatics Engineering courses has been done for six years by the British system.

In the next university analyzed were 5 accredited branches with 3 years in the field of Engineering in Bachelor:

a. Information Technology
b. Computer Engineering
c. Electronic Engineering
d. Mechatronic Engineering
e. Electrical Engineering

There are 4 accredited 2-year courses in Master program in:

a. Information Technology
b. Computer Engineering
c. Electronic Engineering
d. Mechatronics

What is noticeable is that there is very little coverage of the information security field in this university. Only in the Master of Science course, in the second year, there is a subject that is only studied if the students choose it, called Information Security. This course has 60 hours of which only 15 hours are laboratories. In this university students have PCs but Internet problems and computer settings make it impossible to implement security information at these laboratories.

Accreditation of Computer Engineering courses has been done for five years by the British system.

In this university are noticeble two aspects:

a. Lack of staff to cover the information systems
b. Lack of capacity to cover the security of information

In the sixth university were 3 study branches, respectively:

- Applied Informatics
- Information Engineering
- Electronics

Meanwhile, for the first time this year, a master level in computer science has been opened. The number of new students enrolled in the bachelor level in this academic year is 18 students, of whom 15 are boys. Meanwhile, the total number of students in the bachelor level who study in the above fields is 51 students, with 44 being boys. What is noticeable in these programs is that the information security focus at this university is very rare. The number of students enrolled in the master level is only 11 students out of which 8 are boys. Meanwhile in the professional master level only one subject has some elements of information security. This subject is called Information and Business Management Systems. Otherwise, in the syllabus of this subject can be found aspects in the field of business organization and very little, about 5% of security information concepts.

Accreditation of Applied Computer Engineering, Electronics and Informatics has been done for 6 years by the British system.

Laboratories are equipped with new computers, but the infrastructure needed to set up a professional cyber security level is still far from what can be called a professional.

Generally, the number of pedagogues at this university is small and the competence in the field of security is low.

In the seventh university was this situation as below:

The bachelor level in Applied Informatics has been opened at this university. From the analyzis of the programs has been noticed that information security has no dedicated topics.

The university is equipped with two labs with old computer equipment and most of them are unusable by students. There is no internet and there is no decent infrastructure to professionally develop information system curricula. The number of students in bachelor level in Applied Informatics is 61 students, 41 of whom are boys**.**

In the academic year 2018-2019 17 students were registered, 11 of them boys.

Although this university has received accreditation for three years from the British system, there is little chance to implement information security at this university, as the staff at this institution is new but unqualified. **The number of students adhering to the information security field is 0 (zero), as there are no licensed branches in this direction at this university**

In the next university analyzed were opened this year these courses:

• Information Engineering
• Electronic Engineering
• Industrial Engineering

In this University there is an accredited 6 year course in Business Informatics. Also this year at this university is opened the new branch of Security of Information Systems in the Master Professional level, **which unfortunately this year had no students registered. Meanwhile, in the bachelor level in Computer Engineering, Electronics and Industrial Engineering, there are a total of 21 students enrolled, of whom 11 are boys. Meanwhile, in bachelor level of business informatics there are 36 students, 17 of whom are boys, and in Master level in business informatics 25 students, 12 of whom are boys.**

From the observation made at the university premises, and from conversations with the staff, it was found that this university has built three laboratories with computer network and internet but there is, however, no professional infrastructure to create student profiles to be able in the future in the market of the cyber security experts.

Security of Information Systems in the Professional Master level has several subjects on information security such as: Risk Management in IT, Cryptography and Ethical Hacking.

In total, the security field at this department, without including the Information Security System branch in the Master Professional level, covers about 5% of the topics.

However, there is a lack of staff and professionals in the field of information security as in every university.

In the first college is organized a two-year course of professionals in the field of:

a. Information Technology
b. Electronics
c. Industrial
d. Data Base and Web Design

In this academic year, this college enrolled 126 young students, of whom 88 are boys. In total, there are about 276 students in this college, out of which 171 are boys. There are more professionals in this college than pedagogues, because of the low profile that it has. In this college there are 4 laboratories with 25 PCs connected to the network and with a continuous internet. Network maintenance is maintained by a dedicated IT staff. Also in one lab are real equipment with RACK, 4 Servers, 3 Switches Layer 3, a Firewall and a QNAS to enable Cloud. **The security field at this college covers about 15% of the topics.**

The level of infrastructure in this college is the best from all private and public universities in Albania.

In addition to internal professionals there is a network with external professionals connected to this college.

Regardless of the very good infrastructure, the programs and the subject curricula are not very related to the security of information. Only one module is distinguished in the second year, which is related to Information Security.

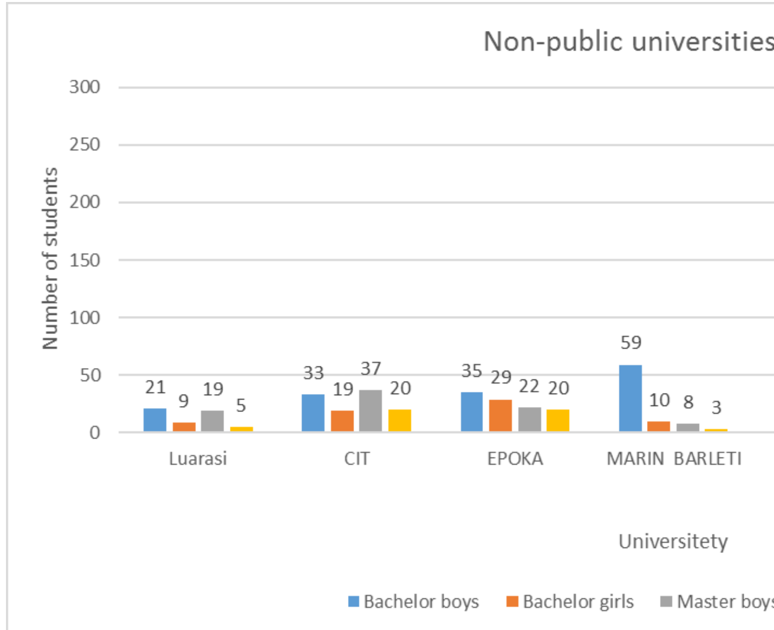

Figure 8 Students in non-public universities

ANNEX 3: ANALYSIS OF STUDY BRANCHES AT TRAINING PROVIDER LEVEL

The first course center analyzed provides Online Training in Practice, run by experienced instructors, which students can attend from their home's comfort. Its experts / instructors work in private or public companies and convey their expertise to the students of the Center.

This course center is classified as an institution of practical knowledge teaching, and follows the "Hands on" approach. **The average annual number of registered people varies from 60 to 80 registered, where about 60% are boys. However, the security field in this course is only about 10% of the above mentioned topics.**

Some of the modules of this center are: Cisco Computer Networks, Windows Server, SQL Server, Linux Server Administration, Java, Phyton etc.

What was found at this center was the lack of cyber security courses such as Penetration testing, Ethical Hacking, Mobile Hacking, Web Hacking, Wireless Security and Auditing. The reason for not opening up to date information security centers is directly related to the lack of instructors and competent staff in this field.

The second course center analyzed is specialized information technology center with a group of qualified trainers. The modules provided at this course center are:

- Cisco
- Java
- Linux
- Microsoft, and
- Oracle.

Even in this center, there are no information security modules. The main reason here is also the lack of trainers, despite the fact that the center itself has high demands from the trainees for this discipline.

The third course center has been licensed for years to provide professional courses in Albania in the field of information technology. Regardless of old equipment and non-illuminated halls in this center, there are developed many modules like Cisco, Java, Linux and Microsoft, but lack information security that is directly related to lack of trainer.

The number of people enrolled in this center in annual terms varies from 90 to 120 per year, with around 55% of them being boys. Only 10% of the topics dealt with in this course center are related to information security.