



Viti i XVI-të i Botimit, Nr.2
Dhjetor 2024

SISTEMI E-ALBANIA KËRKON ADRESIMIN E SFIDAVE PËR TË MBROJTUR TË DHËNAT SENSITIVE TË QYTETARËVE. ËSHTË THELBËSORE TË KRIJOHET NJË SISTEM I SIGURT DHE I BESUESHËM

Valbona Cinaj*

**Albanian University, Tirana, Albania*

Përmbledhje

Përparimet e fundit në teknologji kanë revolucionarizuar proceset tradicionale administrative, duke lejuar ofrimin më të shpejtë dhe më efikas të shërbimeve. Në ritmin e shpejtë të zhvillimit dhe lehtësisë me të cilën informacioni mund të transmetohet, siguria e informacionit është bërë një shqetësim thelbësor për pothuajse çdo organizatë. Si rezultat, organizatat janë të detyruara të përshtaten me këto tendenca dhe të eksplorojnë mënyra për të menaxhuar sigurinë e informacionit në mënyrë efektive. Mekanizmat kryesorë që janë thelbësorë në këtë drejtim përfshijnë politikën, procedurat dhe standardet, të cilat u mundësojnë organizatave të krijojnë një mjedis të sigurt për operacionet e tyre dhe të mbrojnë asetet e tyre, veçanërisht informacionin e tyre të vlefshëm. Ky punim synon të shqyrtojë aspekte të ndryshme të sigurisë së informacionit në institucionet e sektorit publik në Shqipëri, duke përfshirë sfidat dhe mundësitë me të cilat përballen në parandalimin dhe trajtimin e shkeljeve të sigurisë. Për më tepër, ky dokument eksploron se si këto organizata mund të përputhen me standardet ekzistuese, të zbatojnë praktikën më të mira dhe të hartojnë politika për të përmirësuar pozicionin e tyre të sigurisë së informacionit. Me interes të veçantë është perspektiva e punonjësve të IT-së për çështjet e sigurisë dhe shkalla në të cilën këto mekanizma zbatohen brenda organizatave të tyre përkatëse.

Fjalë çelës: *siguri, sisteme informacioni, menaxhimi, teknologji*

IMPLEMENTING AN E-GOVERNMENT SYSTEM IN ALBANIA REQUIRES ADDRESSING CHALLENGES TO SAFEGUARD SENSITIVE CITIZEN DATA. IT'S CRUCIAL TO ESTABLISH A SECURE AND RELIABLE SYSTEM.

Prof. Assoc. Dr. Valbona Cinaj from Albanian University in Tirana, Albania, has written an informative paper examining the various aspects of information security in public sector institutions in Albania, including the challenges and opportunities they face in preventing and addressing security breaches. It also explores how these organizations can comply with existing standards, implement

best practices, and draft policies to enhance their information security posture. The paper also focuses on the perspective of IT employees on security issues and the extent to which these mechanisms are implemented within their respective organizations.

Abstract

Recent advancements in technology have revolutionized traditional administrative processes, allowing for faster and more efficient service delivery. In light of the rapid pace of development and the ease with which information can be transmitted, information security has become a crucial concern for nearly every organization. As a result, organizations are compelled to adapt to these trends and explore ways to manage information security effectively. Key mechanisms that are essential in this regard include policies, procedures, and standards, which enable organizations to create a secure environment for their operations and protect their assets, particularly their valuable information. This paper seeks to examine the various aspects of information security in public sector institutions in Albania, including the challenges and opportunities they face in preventing and addressing security breaches. Additionally, this paper explores how these organizations can comply with existing standards, implement best practices, and draft policies to enhance their information security posture. Of particular interest is the perspective of IT employees on security issues and the extent to which these mechanisms are implemented within their respective organizations.

Keywords: *Security, Information Systems, Management, Technology*

1. Introduction

The use of information systems has become an integral part of our daily lives, with individuals seeking information on a variety of topics from numerous sources. However, in businesses, organizations, and academic institutions, information is used to make decisions and solve problems. The security of information systems in the public sector is crucial, as they often deal with sensitive data or are part of critical infrastructures. In most countries, the public sector includes various levels of government, institutions, and organizations that play significant roles in economic and social development. However, incidents such as the publication of sensitive data for Albanian citizens can be detrimental and must be addressed by implementing strict protocols and guidelines for handling personal information. It is also vital to educate the public on the importance of protecting their data to prevent such incidents from occurring in the future.

2. Literature review

The public sector is generally characterized by the lack of economic markets for their final products [(Bozeman & Bretschneider 1986)]. Then there is the support that this sector has from the government for financial resources. This support produces another limitation, political influence. Different forms of accountability may be necessary that are not typically practiced by private sector firms [(Rainey & Steinbauer, 1999)].

It should also be noted that information systems planning, development, operation, and management in public sector organizations take place in a very specific context that presents particular challenges. Public sector organizations are often burdened with inflexible procurement, employment, reward, and pay procedures and operate within an institutional framework that is not easily changed. These factors

contribute to several issues and difficulties related to information system security in the public sector. Public institutions are required to keep accurate records to maintain internal controls and protect corporate assets against unauthorized use. In addition to the more traditional list of assets such as plant, land, equipment, cash, and people, the list of corporate assets also includes information that is used to support the business or organization. The company's physical assets are protected because lost or damaged assets hurt the company's chances of success. In the same way, by protecting the company's information assets we increase the chance of success. Taking care of asset security improves value by providing a better competitive position in the industry and improved customer service [(Peltier, 2004)].

The growing need to maintain national security eventually led to more complex and technologically sophisticated computer security safeguards [(Whitman & Mattord, 2011)].

There have always been various omissions in terms of safety, especially when dealing with new products that have not been used before. Thus according to [Nayak & Rao (2014)]

The value that information provides is great and must be used with great care by enterprises and organizations to do business and develop in the market. Information systems are of great importance in enterprises and organizations because they can lead to the change of strategy that may occur due to major changes in the market, including market conditions, and especially rapid technological developments. Companies do this to follow the competition or to create a competitive advantage in the market (Laudon, 2014).

Threats to Information According to Whitman & Mattord (2011) a threat is a category of objects, persons, or other entities that pose a risk to an asset. Threats are always present and can be intentional or unintentional. Internal threats and external threats are the two main groups of network security threats. Insider threats are threats from someone inside the organization who has appropriate access to the network and network resources, who has a good understanding of the network infrastructure, and who understands security applications and security holes. External threats are threats from people outside the organization. They do not have authorized access to network resources.

They act by attempting and gaining unauthorized access to the network and network resources to damage the resources or for profit [(Nayak & Rao, 2014)]. Advanced Persistent Threat and Cyber Attacks and different types of threats are evolving rapidly, with the rise of highly organized and funded groups capable of executing persistent attacks. to achieve long-term goals, including cyber-espionage and cyber-terrorism. The rise of organized crime online is entirely logical. Given that money and information are now exchanged over the Internet, organized crime has followed suit, focusing on the theft of valuable assets such as intellectual property (Harkins, 2016).

3. Methodology

1. The method followed in the data is through a case study related to the case of the release of data in Albania for Albanian citizens. These released data affected everyone's life as well as a fundamental violation of human rights.
2. Referring to the situation created in the connection where everyone's data is in everyone's hands, it is the duty of all institutions and the government to take immediate steps to deal with the problem and immediate recovery. It is obvious that now the data have come out and they are still today after so long in everyone's hands and this is an event that has no measure for the negative impact created today and in the future where these data exist in the hands of ordinary citizens. Regarding the importance of protecting the data, a questionnaire was built with a sample of n=80 and it is distributed electronically to

qualified experts who operate in the largest organizations that operate in Albania, whether private or public. To help with the findings made in this chaotic data release situation, semi-structured or open questions have been formulated in the form of opinions from the best IT and cyber security experts.

4. Information systems E - Albania

It is truly wonderful to learn about the triumph of the e-Albania portal.

This resource appears to be an incredible asset for individuals seeking electronic services offered by public institutions in Albania. The fact that it is administered and developed by the National Agency of Information Society provides a sense of security, indicating that the portal is being meticulously managed and maintained. The platform’s future evolution is certainly something to keep an eye on.

e-Albania is a cutting-edge government portal that extends a comprehensive array of online services to the citizens and businesses of Albania. Some of the services that are available on the platform comprise electronic tax filing, online payment of utility bills, access to public records, and an assortment of other government services. Moreover, the portal offers valuable information on government policies and initiatives, news and events, and other resources related to public services. The primary objective of e-Albania is to deliver a more streamlined and transparent government service, mitigating bureaucracy and the need for physical presence in government offices.

E- Albania is a one-stop office for public administration online services
Is an online channel for providing public services 24 hours a day, 7 days a week
Offers electronic services of levels 3 and 4 (according to UNPAN 2014) through the latest technology standards, possibility to make online payments for these services through debit and credit cards
Offers electronic services of levels 1 and 2 (according to UNPAN 2014), where anyone interested can receive detailed information about services for the public, (licenses, permits, authorizations, documents equipped with a digital stamp, certificates, or other services similar), the necessary documentation, the procedure that must be followed, the operating hours and the location of the administration offices, contacts, as well as the address of the official website of the institution that offers the relevant service, where it can be oriented for further details
Is in full compliance with government policies in the field of ICT and the Cross-Sectoral Strategy “Albania’s Digital Agenda 2015-2020”
Provides communication opportunities for any ambiguity, question, or problem regarding registration, the services offered on the portal, through the portal forum, e-mail, comments, and messages on social networks
Has improved the provision of services, reducing the time of receiving the service, avoiding bureaucracies, as well as reducing corruption
Provides information and electronic services that are created and maintained by various public and private institutions.
The availability and accuracy of the service is the responsibility of the responsible institution, which provides its electronic service through the portal
To be the main channel for receiving online public administration services for citizens, businesses, and public administration employees themselves, to offer users a platform where they can be an active part of improving public services and drafting government policies

To expand the user experience through the continuous addition of electronic services with more than 100 other electronic services within the year 2017, to increase the information on the existence of public administration services to all Albanian citizens
Ensures 24/7/365 availability with over 99% portal functionality
Is connected to the Government Platform of Interaction (Government Gateway), in which 48 systems are connected which exchange data in real-time
The interaction system is a multifunctional central system, an Enterprise Service Bus solution with a service-oriented architecture
Payments for electronic services are made securely through the Government Electronic Payments Platform, which is connected to banking and non-banking institutions
Offers the integration of a variety of security technologies to protect user data. The registration process is carried out through the government portal and the data filled in by users during the registration process are verified electronically with the data of the National Register of Civil Status for individuals and the National Commercial Register for businesses (CKB
The authentication and identification process is based on the “Single-Sign-On” strategy, to create a unique identity for each user, using NID for citizens and NUIS for businesses
Is compatible with the latest versions of Internet browsers such as Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc.
Accessible in mobile web, iOS, and Android mobile app versions
It is offered 100% in the Albanian language;
E-Albania is a secure system and is not related to any leakage of information.
Precisely for the registries to interact safely, the governmental interaction platform was built, which makes it possible to have no exports, but the systems to communicate with each other in real time and automatically, without people from behind.
The 17 million transactions of this platform that are made every month, in addition to reducing all the generating documents that the citizens and businesses need, are carried out securely, leaving clear logs. The platform is maintained by Microsoft, which enables full security

5. Case study. The case of the publication of sensitive data for Albanian citizens

In April 2021, a few days before the general elections in the country, a database with the private information of around 910,000 voters in Tirana was leaked to the media.

It was claimed that the database belonged to the ruling Socialist Party and was taken from state institutions and used for electoral purposes. The database, which BIRN¹ has seen, contained some 910,000 entries including names, addresses, birth dates, personal ID cards, employment information, and other data.

The Socialist Party denied wrongdoing, insisting that the information was gathered in door-in-door surveys. After some months another database containing the personal data of hundreds of thousands of Albanian citizens which has been circulated on social media.

It is alleged that the data contains the monthly salaries, job positions, employer names, and ID num-

1 Balkan Investigative Reporting Network

https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://birn.eu.com/&ved=2ahUKewj65dOqwZmFAxWe2AIHHeEdDEcQFnoECACQAQ&usg=AOvVaw0Lzlt_fjE_Bq6lLwqcBCHH

bers of some 630,000 citizens, from both the public and private sectors. It is suspected that the list was leaked from the tax service or the Social Insurance Institute.

A government spokesman said that the Ministry of Finance was following up with concern about the release of data on the salaries of Albanian citizens, and described the document as “illegal”.

In Albania, several databases with the personal data of hundreds of thousands of Albanian citizens, such as salaries, ID card numbers, and vehicle license plates, the number mobiles are circulating on WhatsApp and social networks.

The information that came from the General Directorate of Taxes told that suspected to be the source of the leakage of the payrolls, he found that this institution did not have the appropriate standards for the protection of personal data. Experts and journalists say that the prosecutor's office, which has launched an investigation into the criminal offense of «Misuse of personal data and Abuse of duty», has sufficient evidence to investigate other criminal offenses such as money laundering, corruption and fiscal evasion.

After circulating on the WhatsApp social network, the three databases, two with the payrolls of 630,000 thousand Albanian citizens, and one with car license plates. Legal and national security experts emphasized that the disclosure of salaries and other personal data such as identity card numbers constitutes the biggest scandal of all time in the field of personal data in Albania. “This is not a random leak of information since, as you saw, the first list came out, a more reduced list, the prime minister came out to give explanations, and another detailed list came out.

This process leads to collapse, and this requires an urgent undertaking. Below we are giving a table of this database that is circulating and today even their number has been added. We are referring to the findings of some indicators obtained in the processing of this database.

	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Muhamet Haxhiu	Muhamet			3:00 AM	Durrës		70,000.00	Administrator	I punësuar me kohë të plotë ose të pjesshme c				
2	Emri	Mbiemri	EMRI I PUK NIPT		Subjekti	DRT		Paga Bruto	Profesioni	Kategoria				
3	Anonymo	Anonymo	Anonymo J92113001		SHERBIMI INI	Tiranë		58,074,817.00	Papercaktuar	Papercaktuar				
4	Ben	Blushi	Ben Blush K1200700		TOP CHANNE	DTM		24,756,130.00	Drejtor i përgjith	I punësuar me kohë të plotë ose të pjesshme c				
5	Anonymo	Anonymo	Anonymo K5171305		DREJTORIA SI	Tiranë		9,285,761.00	Papercaktuar	Papercaktuar				
6	Sadik	Ismailaj	Sadik Ism L6240503		FINMAN	Tiranë		8,510,061.00	Sipërmarrës	I punësuar me kohë të plotë ose të pjesshme c				
7	Idajet	Ismailaj	Idajet Ism L6240503		FINMAN	Tiranë		8,510,061.00	Sipërmarrës	I punësuar me kohë të plotë ose të pjesshme c				
8	Michael	Smith	Michael S L2180700		Shell Upstres	DTM		6,555,621.00	Kontabilist	I punësuar me kohë të plotë ose të pjesshme c				
9	Anonymo	Anonymo	Anonymo K5290522		SHERBIMI INI	Elbasan		6,528,303.00	Papercaktuar	Papercaktuar				
10	Anonymo	Anonymo	Anonymo K5782954		SHERB.INFOR	Lezhë		6,449,679.00	Papercaktuar	Papercaktuar				
11	Mentor	Petrela	Mentor P K6182100		AMERICAN H	DTM		6,360,949.00	Kirurg në neurok	I punësuar në dy subjekte (I dypunësuar) kur s				
12	Anonymo	Anonymo	Anonymo K9403059		SH.I.SH. DREJ	Fier		5,811,335.00	Papercaktuar	Papercaktuar				
13	Anonymo	Anonymo	Anonymo K6231001		KORPUSI I PA	Tiranë		5,614,483.00	Papercaktuar	Papercaktuar				
14	Eduard	Curraj	Eduard C K6220204		DELTA PHARI	DTM		5,577,915.00	Drejtor ekzekutiv	I punësuar me kohë të plotë ose të pjesshme c				
15	Illa	Jorgji	Illa Jorgji K0312460		ELKA-SA	DTM		5,569,282.00	Drejtor i përgjith	I punësuar me kohë të plotë ose të pjesshme c				
16	Anthonie	Frens	Anthonie L2180700		Shell Upstres	DTM		4,732,187.00	Administrator	I punësuar me kohë të plotë ose të pjesshme c				
17	Peter	Francis	Peter Fra L5181600		BRUNEL ENER	DTM		4,503,007.00	Manaxher projek	I punësuar për herë të parë apo rishtazi te subj				
18	Bozhidar	Todorov	Bozhidar T K7201480		Banka e Parë	DTM		4,474,258.00	Drejtor i përgjith	I punësuar me kohë të plotë ose të pjesshme c				
19	CHRISTIAN	CANACAR	CHRISTIAN J6191100		RAIFFEISEN B	DTM		4,368,654.00	Drejtor i përgjith	I punësuar me kohë të plotë ose të pjesshme c				
20	Zeljko	Miric	Zeljko Mir L6190106		COCA-COLA E	DTM		4,225,600.00	Drejtor në shërb	I punësuar me kohë të plotë ose të pjesshme c				
21	Denis	Kelleher	Denis Kell L2180700		Shell Upstres	DTM		4,078,912.00	Inxhinier shpimi	I punësuar me kohë të plotë ose të pjesshme c				
22	Anonymo	Anonymo	Anonymo K4312864		DREJTORIA R	Gjirokastrë		4,055,900.00	Papercaktuar	Papercaktuar				
23	Kristina	Naumi	Kristina N K9162402		Tranzit	Tiranë		4,051,400.00	Administrator	I punësuar me kohë të plotë ose të pjesshme c				
24	Petrit	Maho	Petrit Mal J7142402		I N T E R M E	DTM		3,978,227.00	Administrator	I punësuar me kohë të plotë ose të pjesshme c				
25	SILVIO	PEDRAZZI	SILVIO PE L8181700		INTESA SANP	DTM		3,916,195.00	Drejtor shërbime	I punësuar me kohë të plotë ose të pjesshme c				

Table 1 Table of the salary list of citizens in Albania that are public on social media and WhatsApp.

There are 630,000 citizens, from both the public and private sectors. The fields that are complete

In the field begin with the ID, name, surname, name, and surname (it is written in red), the NIPT of the entity where the salary is received, the name of the entity where you work, the location as well as the gross salary received (it is written in red) to continue with the column of the job position he holds as well as the full-time or part-time status.

This circulating database is a reference and we can be drawing some conclusions

First, we calculate the average salary in Albania by referring to the data published through Excel *it would be =AVERAGE (H3:H523349), and through this function of Excel, we calculate the **average salary in Albania**, which in fact according to the declared data turns out to be

52,403 ALL².

For further statistical analysis, we also use the percentage, which signifies a statistical measure that shows the value below which a certain percentage of observations in a group of observations falls, for example,

this function shows us the value of the salary that has less than 75 % of citizens =PERCENTILE (H3:H523349,0.75),

the value of this function is **60,870 ALL³**,

so 25% of them have salaries **higher than 60,870 ALL**.

Variance and Standard Deviation are the two important measurements in statistics.

Variance is a measure of how data points differ from the mean, while

standard deviation is a measure of the distribution of statistical data.

Furthermore, it is convenient to measure how much salaries vary relative to the mean. For this purpose, we calculate the standard deviation and variance with the **auxiliary function STDEV and VAR.P**.

We first calculate the standard deviation through the formula =STDEV.S(H3:H523349)

this function from which the **value 113.384 comes out**, so this is the number of salaries that differ from the average.

Continuing further with the variance function from which =VAR.P(H3:H523349) we calculate **the spread of the data around its mean value**.

Referring to all citizens, they must protect themselves and be careful. Many problems with institutions, to social problems in the entire population. Problems and challenges for the management of this system and the challenges that arise to standardized nowadays where we are officially candidates for part of the integration in Europe.

As a country that wants to become part of Europe, we must also respond to the standards of the institutions that deal with this information and sensitive data for Albanian citizens.

Questions that arise about this situation are some as below

1. Why is the release of a payroll from almost a year ago happening now?
2. What purpose is hidden behind this act, which was also followed by the publication of a database with car license plates of Albanian citizens?
3. Is it a concern that should be considered for national security?

2 Albanian currency

3

4. Are there other sensitive data that can be released later according to a structured plan?
5. If there will be other data, is an organization facing a certain goal, which aims to either shift attention from an important investigation or other essential problem or to create a destabilizing situation in Albania
6. Are persons protected in Albania?
7. Should the publication of personal data be considered, the responsibility for the violation of the legislation? There may be other questions as derivatives of those raised above, but we are limiting ourselves here.

Conclusions of the case study

Dealing with the situation seriously is not done with justifications of improving the work with control groups or with other findings, because if the accessory is not stopped, then all the data will be released to the public. Therefore, the system must be ensured,

The Commissioner for the Right to Information and Protection of Personal Data considers the publication of the salaries and ID card numbers of hundreds of thousands of citizens a serious event and says that an administrative investigation has been launched.

The necessity of improving security management systems, the need to increase the budget for the protection of personal data, as well as the preparation of experts in this field, should be considered immediately.

Such a gap and publication in the published database that is in everyone's hands promotes numerous social problems that harm businesses that are the promoters of the economy.

The publication of personal data in Albania highlights the weaknesses of the institutions.

Many citizens, with the publication of data, risk being targeted by criminal groups.

And to be used by them

Many citizens referring to their high salaries can hide affairs and corrupt acts., for the effect of what we usually call 10, 15, or 20 percent of tenders. There is a possibility that in these companies. with such high salary levels, employers should agree with employees of the type "I will set the salary at 3 million. O

f these 3 million, you take one, you will return the rest". And then this money is used for bribes. It finds certain companies which on the one hand come out with a negative balance, and on the other hand, have high salaries.

For the Albanian level of wages, some salaries surprised, and here there are full indications have investigations for certain companies for the criminal offense of money laundering.

So are other companies that can be investigated for concealment of income and tax evasion.

The Commissioner for the Right to Information and Protection of Personal Data as well as experts say that administrative and criminal sanctions for extracting personal data are negligible concerning the damages, and add that they should be strengthened.

Great achievement digitization of services, must be accompanied by strong security measures. The

release of citizens' data from the government information system in Albania

6. Analysis of a survey for the senior level of IT employees (selected with mostly open questions) n=80

Referring to a simple survey conducted mainly with high-level IT specialists, we came up with some findings. A survey of 80 representative people in large private and government businesses has the following:

1. Regarding the information security strategy, the majority of IT employees (52.4%) answered negatively, i.e. that the organization they work for does not have a documented security strategy. However, many of these organizations have other documents, security policies, or general policies for the use of IT equipment and services.

2. Referring further to the findings of the survey, it can be seen that a large number of organizations do not have any documented information security strategy, as the main document related to this field. However, many of these organizations have other documents, security policies, or general policies for the use of IT equipment and services. So we understand what are the main areas addressed through the existing documents that issues and requests related to passwords are addressed in 95.2% of cases. Whereas other issues such as the use of the Internet and e-mail are addressed in 90.5% of cases. Issues that are still not sufficiently addressed are data classification and information storage/destruction (after a certain time).

A large increase in the use of mobile devices has also been noted, therefore not regulating this field can be problematic for these organizations since based on the answers we understand that about 61.9% have addressed mobile devices through official documents. From this, we notice that even mobile devices still do not have adequate handling of these documents.

- It can be seen that the majority of employees appreciate that there is adequate security in the buildings and locations of their organizations. But there are also a small number who do not appreciate this very important aspect of security.

- It is known that one of the primary aspects of security is denying physical access to certain devices to persons who are not authorized to work with them. Also, another aspect is the issue of cables which must be placed in safe ways to avoid the possibility of intentional or accidental damage.

Employees have assessed that the placement and protection of equipment and cables is adequate but generally not at a satisfactory level. This can be justified considering the different nature of the organizations.

We have organizations that operate in modern facilities and locations that have been built in recent years, or in facilities that have undergone renovations and adjustments in terms of networks and infrastructure. While a part of the organizations also operates in private facilities which do not meet the conditions they should in terms of security issues.

The rest of the organizations operate in public facilities but possess outdated infrastructure or have deficiencies in this regard. Another aspect is the control of access to the computer network. Here the respondents gave mostly positive answers, implying that there are adequate controls that prevent unauthorized persons from accessing the organization's computer network. While network access can be controlled by various methods including physical ones, this can be more problematic when it comes to Wireless networks. It is known that the use of Wireless networks is a particular challenge for many organizations when we consider the easier possibility of accessing them compared to wired

networks.

- A significant number of respondents stated that the organization they work for specifies safety obligations for its employees. Some of them (28.6%) have no information about this, and 19% answered negatively. This is a very important issue since employees are the ones who have access to various information and not clearly defining their duties and obligations regarding information security can result in security incidents.

- As for contracts with external parties, it is a different picture. Where a large majority of organizations specify security requirements to external parties. However, even here there is room for improvement, knowing that external parties do not always have good intentions when they enter the organization's premises. This is especially true for many organizations that have multiple services that are outsourced.

- It is known that organizations differ from the smallest to the largest, in this respect, the responsible personnel who deal with security issues also differ. The largest number of respondents have emphasized that the main persons responsible for security are the Network Administrator or the System Administrator. While a smaller number have emphasized that this field is covered by an IT Specialist or, in the best cases, an Information Security Specialist. In this respect, the situation is not ideal because it is known that the staff who perform other important functions find it difficult to fully dedicate themselves to security issues. Only a certain number of larger organizations have the possibility of delegating this responsibility to a dedicated person or department.

- The most frequently used ways to increase awareness regarding information security seem to be the general ones that also include verbal forms. While a smaller number distribute relevant news from time to time. Several people have stated that they try to achieve this by complying with different standards and policies. Here too we note that the organization of training for certain groups is not one of the priorities of these organizations. Another aspect addressed is the evaluation of the efficiency of information security management. The majority of respondents (57.1%) answered that an assessment regarding efficiency is made by the IT staff/department. A smaller part (19%) stated that such evaluation is done by the internal audit. While 33.3% have emphasized that no such assessment is made at all regarding the efficiency of information security management.

- One of the key aspects that is also described by many different standards that have been mentioned above is the management of incidents. Knowing this, the question was asked whether the organization has written procedures for the management of security incidents, which was answered positively by less than half of the respondents. This is a major concern knowing that the lack of written procedures leaves the door open for such incidents and creates major obstacles in restoring service when they do occur.

- The Continuity Plan of the business or organization is certainly difficult to imagine without a Disaster Recovery plan or strategy. About 47.6% of respondents answered positively to this question. This can also be explained by the nature of some smaller organizations which may have carried this responsibility to a larger supervisory organization. However, regarding the way organizations evaluate such a plan, most have answered that this is done through a partial simulation of the restoration of certain backups. Another part stated that such an evaluation is not performed at all and that this can be very problematic if a previous backup needs to be returned and it does not work because it has not been tested in advance. While no response has been received to the option of simulating emergencies, i.e. organizations do not practice this method.

- The application and implementation of internationally accepted standards are still not present in public organizations. Based on the responses received, it appears that most organizations do not use any specific standard. Several answers have emphasized the use of any other standard, other than

those listed (which are part of the set of the most popular standards). The second part of Figure 12 is the question related to the implementation and use of ISMS, the Information Security Management System. Even in this area, most organizations have not implemented ISMS. However, the largest number of respondents stated that the possibility of implementing ISMS has been considered and will probably be considered again. A smaller part stated that the use of ISMS was never thought of and considered as an option. While some of the respondents stated that ISMS is used in certain organizations.

8. Conclusion

Through the conducted research, we can reach some conclusions regarding information security and its management in public sector organizations. The results show that despite many areas where there is an adequate handling of security issues, there are also areas that require improvement.

The conclusions and recommendations in this case are more general than specific to certain organizations. One of the main aspects is the design and development of policies and procedures. Greater investment in this direction would affect the clear establishment of responsibilities for all activities related to information security. Written procedures would not leave much room for ambiguity regarding the handling of incidents or other areas of security. Here I believe that better coordination is needed with management and relevant legal officials so that they have as clear as possible the importance of policies and procedures in IT because there are cases when these officials are not so familiar with procedural issues in IT. This is when it is known that a certain part of the management in these organizations is political and not always interested in the smooth running of certain processes.

Another area for improvement is to better address the issue of information classification. Utilizing a more coherent classification, the management of information would be facilitated, especially where sensitive information is concerned. The organization of pieces of training for users is another aspect that has room for improvement. This is because information security issues are often not taken seriously by users. In this direction, organizations can perhaps use the existing infrastructure of training institutes in the public sector.

The assessment or evaluation of current practices in IT in general but also in information security needs significant improvement. This is because, based on the answers, we have understood that often such evaluations are made by the employees themselves, or in other cases they are not made at all.

In the above-mentioned field of assessment of practices and processes implemented in IT, the audit of IT processes would play an important role. This field is still in its initial phase in our country, always referring to the public sector. Audits carried out so far by external auditors are mainly focused on regularity and financial issues. With the development of IT audit (part of this would also be the issue of information security) an opportunity would be created to influence the practices implemented in IT. Through recommendations and alignment with standards or good practices, better security management would be ensured. This would also be of great help to IT staff in various organizations as they would be more up-to-date with these practices. Another issue more specific to the public sector is the procurement of IT equipment and services. This often affects the creation of certain situations where an organization can be left without a certain service or device (affecting security) for a certain time, therefore very precise planning of these activities is required to avoid reaching the point where endangers the safety

Reference

- [1] Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security* (4th ed.). Boston, MA: CENGAGE Learning Custom Publishing.
- [2] Nayak, U., & Rao, U. (2014). *The Infosec handbook: An introduction to information security*. Germany: APress.
- [3] Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing*. United States: Prentice Hall.
- [4] Rhodes-Ousley, M. (2013). *Information security: The complete reference*, Second edition (2nd ed.). New York: McGraw Hill Education.
- [5] Alexander, D., Finch, A., & Sutton, D. (2013). *Information security management principles* (2nd ed.). Swindon: BCS, The Chartered Institute for IT.
- [6] Peltier, T. R. (2004). *Information security policies and procedures: A practitioner's reference*. Boca Raton: Auerbach Publishers.
- [7] Landoll, D. J. (2016). *Information security policies, procedures, and standards: A practitioner's reference*. United States: Auerbach Publishers.
- [8] Axelrod, C. W., Bayuk, J. L., & Schutzer, D. (Eds.). (2009). *Enterprise information security and privacy*. Boston: Artech House Publishers.
- [9] Bosworth, S., Kabay, M. E., & Whyne, E. (2014). *Computer security handbook* (6th ed.). United States: John Wiley. I
- [10] Schlienger, T. & Teufel, S. (2002). Information security culture: the socio-cultural dimensions in information security management". In Ghonaimy, M. A., El-Hadidi, M. T. and Asian, H. K. (eds). *Security in the Information Society: Vision & Perspectives*, Kluwer Academic.
- [11] Ward, J. (2002). Developing a culture of information security. Proceeding of the 19th World Conference on Computer Security Audit and Control, London.
- [12] Zakaria, O. & Gani, A. (2003). A Conceptual Checklist of Information Security Culture, Proceeding of the 2nd European Conference on Information Warfare and Security, MCIL,
- [13] Dowland, P. S. (2005). Security management, integrity, and internal control in information systems: Ifip Tc-11 WG 11.1 & WG 11.5 joint working conference. New York: Springer-Verlag New York.
- [14] Forcht, K.A. (1994). *Computer Security Management*. Massachusetts: Boyd & Fraser.
- [15] Halliday, S. & Von Solms, R. (1995). *An Alternative Approach to IT Risk Analysis and Management*. MTech thesis. Port Elizabeth: Port Elizabeth Technikon.
- [17] Von Solms, R. (1998). *Information Security Management (3): The Code of Practice for Information Security Management (BS 7799)*, Information Management & Computer Security.
- [18] Information Security Management (BS 7799), Information Management & Computer Security.
- [19] Ghonaimy, A. M., El-Hadidi, M. T., & Aslan, H. K. (Eds.). (2002). *Security in the information society: Visions and perspectives*. Boston, MA: Springer US.
- [20] Strous, L. (1998). *Integrity and internal control in information systems: Volume 1: Increasing the confidence in information systems*. Boston, MA: Springer US.
- [21] O'Hanley, R., & Tiller, J. S. (Eds.). (2013). *Information security management handbook*, sixth edition, volume 7 (6th ed.). Boca Raton, FL, United States: Auerbach Publishers.
- [22] Hone, K. and Eloff, P. (2002). Information security policy – what do international information security standards say? *Computers & Security*.

- [23] Harkins, M. W. (2016). *Managing risk and information security: Protect to enable: 2017*. Germany: APress.
- [24] Layton, T. P. (2006). *Information security governance: Design, implementation, measurement & compliance*. Boca Raton, FL: Auerbach Publications.
- [25] Valbona Cinaj and Bashkim Ruseti 2021 *Information Systems Models in the Hotel Industry and Effects on the Economy (The Case of Albania)*, Ovidius University Annals, Economic Sciences Series, 2021, vol. XXI, issue 1, 67-75
- [26] Valbona Cinaj (cinajvalbona@gmail.com) and Rebeka Ribaj ‘*Macroeconomic Impact of Natural Disasters in Albania*’, Ovidius University Annals, Economic Sciences Series, 2021, vol. XXI, issue 1, 59-66
- [27] Valbona Cinaj, 2017 *Sistemet e Informacionit Te Kreditit Ne Shqiperi* by Valbona Cinaj, Trade Paperback)
- [28] Valbona Cinaj 2017 *Sistemet e informacionit te kreditit ne Shqiperi*, Credit Information Systems in Albaniav Valbona Cinaj Häftad Albanska, 2017-04-04