ReSPA

Regional School
of Public Administration

Abuse of Information Technology (IT) for Corruption

ReSPA activities are
financed by the EU

ReSPA
Regional School
of Public Administration

Abuse of Information Technology (IT) for Corruption

ReSPA activities are
financed by the EU

ReSPA is a joint initiative of European Union and the Western Balkan countries working towards fostering and strengthening the regional cooperation in the field of public administration among its Member States. It seeks to offer excellent innovative and creative training events, networking activities, capacity building and consulting services to ensure that the shared values of respect, tolerance, collaboration and integration are reaffirmed and implemented throughout the public administrations in the region.

CONTACT

Regional School of Public Administration
Branelovica
P.O. Box 31, 81410
Danilovgrad, Montenegro

Telephone: +382 (0)20 817 200
Internet: www.respaweb.eu
E-mail: respa-info@respaweb.eu

CIP – Каталогизација у публикацији
Национална библиотека Црне Горе, Цетиње

ISBN 978-9940-37-005-3
COBISS.CG-ID 29075728

Authors

ReSPA

Goran Pastrovic, *Training Manager*

International authors

Introduction, Overviews for Chapters 1 and 2, Subchapter 2.9 & Chapter 3

Tilman Hoppe, *anti-corruption expert*
Vera Devine, *anti-corruption expert*
Louise Thomasen, *eGovernment expert*

National authors

Albania

Edlira Nasi, *anti-corruption expert*
Ened Kercini, *eGovernment expert*

Bosnia and Herzegovina

Aleksandra Martinovic, *anti-corruption expert*
Srdjan Nogo, *eGovernment expert*

Croatia

Zorislav Petrovic, *anti-corruption expert*
Ivana Andrijasevic, *eGovernment expert*

Kosovo*

Hasan Preteni, *anti-corruption expert*
Driart Elshani, *eGovernment expert*

Macedonia

Marjan Stoilkovski, *anti-corruption expert*
Rozalinda Stojova, *eGovernment expert*

Montenegro

Dusan Drakic, *anti-corruption expert*
Ivan Lazarevic, *eGovernment expert*

Serbia

Nemanja Nenadic, *anti-corruption expert*
Bojan Cvetkovic, *eGovernment expert*

* This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ opinion on the Kosovo declaration of independence.

Foreword

By Suad Music,
ReSPA Director

The "United Nations Convention against Corruption" (UNCAC) states in its Article 48 par. 3:

"States Parties shall endeavour to cooperate within their means to respond to offences covered by this Convention committed through the use of modern technology."

Until today, this provision has not received much attention by the work of international organisations. In fact, the Technical Guide on the implementation of UNCAC[1] contains as only guidance the following:

"Paragraph 3 (of Article 48) recognizes the increasing use of computer technology to commit many of the offences covered by the Convention and calls upon States Parties to endeavour to cooperate more closely in order to respond to corruption related offences committed through the use of modern technology."

This Comparative Study aims to provide, for the first time, concrete guidance by showing cases of abuse of "modern technology" (IT) for corruption offences and on the possible steps that can be taken to protect against such abuses.

ReSPA has been active in both fields for years – integrity as well as e-government. With its regional networks of experts on both issues it is in an excellent position to bring both disciplines together for mutual benefit. In light of its relevance for the implementation of the UNCAC, the impact of this Study will affect the Western Balkan region and at the same time go internationally well beyond the region to any of the 172 parties to the UNCAC.

1 By UNODC, 2009, www.unodc.org/unodc/en/treaties/CAC/technical-guide.html.

Contents

Acronyms

The following is an alphabetical list of acronyms and their meanings used in the report.

AI	Administrative Instruction
ASPA	Albanian School of Public Administration
BiH	Bosnia and Herzegovina
CA	Certification Authority (Macedonia)
CARNet	Croatian Academic and Research Network
CCTV	Closed-circuit television
CERT	Computer Emergency Response Team
CIPS	Citizen Identification Protection System (Bosnia and Herzegovina)
COC	Command Operations Centre (Serbia)
CPI	Corruption Perceptions Indices
CSIRT	Computer Security Incident Response Team
CAA	Civil Aviation Authority (Albania)
DDoS	Distributed Denial of Service
DECO	Department of Economic Criminal Offences (Croatia)
DMS	Document Management System
DORH	Municipal State Attorney's Office in Dubrovnik
ENP	Electronic Toll Payment (Serbia)
ERE	Albanian Energy Regulatory Entity
e-SEE	Electronic South Eastern Europe
EU	European Union
EUPM	European Union Police Mission in Bosnia and Herzegovina
FTP	File Transfer Protocol
HAC	Hrvatske autoceste - Croatian Motorways Ltd.
HDZ	Hrvatska Demokratska Zajednica – Croatian Democratic Union
HJCP	High Judicial and Prosecutorial Council (Bosnia and Herzegovina)
HJPC	High Judicial and Prosecutorial Council (Bosnia and Herzegovina)
HNS	Hrvatska Narodna Stranka – Croatian People's Party
HRT	Croatian Radio-Television
HZMO	Croatian Pensions Insurance Institute
ICT	Information and Communications Technology
IDDEEA	Agency for Identification Documents, Registers, and Data Exchange (Bosnia and Herzegovina)

IDS	Intrusion Detection System
IMPACT	International Multilateral Partnership Against Cyber Threats
IPA	Instrument for Pre-accession Assistance (Bosnia and Herzegovina)
ISO	International Standards Organisation
ISP	Internet Service Provider
IT	Information Technology
JPTC	Judicial and Prosecutorial Training Centres (Bosnia and Herzegovina)
MIST	Ministry for information Society and Telecommunications
MLSP	Ministry of Labour and Social Policy (Macedonia)
MoD	Ministry of Defence
MoI	Ministry of the Interior
MoJ	Ministry of Justice
MoJPA	Ministry of Justice and Public Administration (Serbia)
MPALSGHR	Ministry of Public Administration, Local Self Government and Human Rights (Serbia)
MUP	Ministarstvo Unutarnjih Poslova - Croatian Ministry of the Interior
NACS	National Agency on Cyber Security (Albania)
NAIS	National Agency on Information Society (Albania)
NDA	Non-Disclosure Agreement
NFC	Near-Field communication
NGO	Non-Governmental Organisation
OIB	Personal Identification Number (Croatia)
PARCO	Public Administration Reform Office (Bosnia and Herzegovina)
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PRO	Public Revenue Office (Macedonia)
SAI BiH	Supreme Audit Office of Bosnia and Herzegovina
SAI RS	Supreme Audit Institution of the Republic of Srpska
SCPC	State Commission for Prevention of Corruption (Macedonia)
SDH	Synchronous Digital Hierarchy
SDP	Social-Democrat Party (Bosnia and Herzegovina)
SDS	Serb Democratic Party (Bosnia and Herzegovina)
SIPA	State Investigation and Protection Agency
SNSD	Party of Independent Social Democrats (Bosnia and Herzegovina)
SOA	Security and Intelligence Agency (Croatia)

SOP-s	Standard Operating Procedures
SSA	Supreme State Audit (Albania)
SSL	Secure Sockets Layer
TCMS	Total Case Management System (Bosnia and Herzegovina)
TIMS	Total Information Management System (Albania, Serbia)
UNODC	United Nations Office on Drugs and Crime
USKOK	Ured za suzbijanje korupcije i organiziranog kriminaliteta - Croatian Bureau for Combating Corruption and Organised Crime
VM	Veteran Ministry (Croatia)
VPN	Virtual Private Network
VSOA	Military Security and Intelligence Agency (Croatia)
WAN	Wide Area Network

Introduction

By Tilman Hoppe

Numerous publications exist on how corruption can be **prevented** through good use of IT, such as online public registries, transparency of asset declarations, or e-procurement. The following publications are prominent examples of exploring methods of using IT to fight corruption:

- Tim Davies/Silvana Fumega, "Mixed incentives: Adopting ICT innovations for transparency, accountability, and anti-corruption", U4 Issue 2014:4, 38 pages[2]
- UNDP, "Fighting Corruption with e-Government Applications", APDIP e-Note 8/2006, 4 pages[3]
- Spider, "Increasing Transparency & Fighting Corruption Through ICT – Empowering People & Communities", ICT4D Series no. 3/2010, 102 pages[4]
- Spider, "ICT for Anti-Corruption, Democracy and Education in East Africa", Spider ICT4D Series no. 6/2013, 96 pages[5]
- Jamshed J. Mistry/Abu Jalal, "An Empirical Analysis of the Relationship between e-government and Corruption", The International Journal of Digital Accounting Research, Vol. 12, 2012, pp. 145-176[6]
- Ionescu, Luminita, "The Impact That E-Government Can Have on Reducing Corruption and Enhancing Transparency", Economics, Management and Financial Markets, Vol. 8, no. 2, 2013, page 210
- Bertot/Jaeger/Grimes, "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies", Government Information Quarterly Vol. 27 Issue 3, 2010, p. 264
- Richard Heeks, "Information Technology and Public Sector Corruption", Institute for Development Policy and Management, September 1998, 15 pages[7]

2 http://www.u4.no/publications/mixed-incentives-adopting-ict-innovations-for-transparency-accountability-and-anti-corruption/.
3 http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan043296.pdf.
4 http://spidercentre.org/polopoly_fs/1.163640.1390315885!/menu/standard/file/Spider%20ICT4D%20series%203%20Increasing%20transparency%20and%20fighting%20corruption%20through%20ICT.pdf.
5 http://spidercentre.org/polopoly_fs/1.163057.1390315079!/menu/standard/file/Spider%20ICT4D_no6_2013.pdf.
6 www.uhu.es/ijdar/10.4192/1577-8517-v12_6.pdf.
7 http://unpan1.un.org/intradoc/groups/public/documents/NISPAcee/UNPAN015477.pdf.

- Transnational Crime and Corruption Centre, "Transnational Crime, Corruption, and Information Technology", Conference Report 2000, 39 pages[8]

However, for the reverse usage of IT as a **tool for** corruption, little if any literature exists. The Hong-Kong "Independent Commission against Corruption" has published:

- "Ethics at Work – A Guide for Business Managers in the Use of IT", 2003, 77 pages[9], which focuses on the private business sector.
- There are few incidents where anti-corruption bodies have picked up on ICT as being a corruption risk in the public sector. The following are two of the few examples:
- Kenya Anti Corruption Commission, "Corruption Prevention Guidelines on ICT Systems in the Public Sector", March 2008[10]
- Independent Commission Against Corruption (ICAC) of New South Wales – NSW (Australia), "Knowing your risks: IT systems"[11]

The webpage by the NSW ICAC shows only two short case examples on public sector corruption related to IT. Furthermore, the following technical guidance by international organisations on corruption rarely – if at all – mentions IT as a risk:

- UNODC, UN Anti-corruption toolkit (3rd edition 2004)[12];
- UNODC, Technical guide to the UNCAC, 2009[13];
- OSCE, Best practices in combating corruption, 2004[14];
- Transparency International, Confronting corruption: the elements of a national integrity system, TI Source Book 2000[15];
- USAID Corruption Assessment Handbook (2006)[16].

This scarcity of guidance is in stark contrast to the "United Nations Convention against Corruption" (UNCAC) which calls, in Article 48 par. 3, for States Parties to "endeavour to cooperate within their means to respond to offences covered by this Convention committed through the use of modern technology." Thus, a comprehensive regional study on this topic is long overdue.

8 http://traccc.gmu.edu/pdfs/publications/transnational_crime_publications/variou01.pdf.
9 http://www.icac.org.hk/new_icac/files/cms/eng/13857pdf.pdf.
10 www.eacc.go.ke/docs/ICT_Guidelines.pdf.
11 http://www.icac.nsw.gov.au/preventing-corruption/knowing-your-risks/it-systems/4911.
12 www.unodc.org/documents/corruption/publications_toolkit_sep04.pdf.
13 www.unodc.org/unodc/en/treaties/CAC/technical-guide.html.
14 www.osce.org/eea/13738.
15 www.transparency.org/publications/sourcebook
16 www.usaid.gov/our_work/democracy_and_governance/technical_areas/anticorruption_handbook/

The reader of this Study can benefit from concrete cases illustrating how corruption offenders exploit weaknesses in IT structures for their personal advantage. The real life cases of IT corruption, as well as the **good examples** of preventing and detecting them, will provide inspiration to experts dealing with corruption prevention as well as experts in charge of IT security.

This Study focuses only on corruption risks **specifically** related to IT. For example, corrupt procurement of IT or vendor lock-in are corruption risks which can occur with any other tool such as procuring trains for public transportation or possible vendor lock-ins; thus, they are not corruption risks specifically related to IT.

It is expected that ReSPA members will have different approaches and usages of IT and thus will learn from an **exchange** facilitated by this comparative Study. As there is no typology of cases yet in IT or anti-corruption literature, the added value and impact of this Study may go well beyond the ReSPA region.

1. Real life cases of abuse of IT for corruption

Overview

By Tilman Hoppe and Louise Thomasen

The following cases are a random, non-representative selection of cases from the ReSPA region. It is important to underline that the cases outlined have not necessarily been subject to judicial scrutiny by a court; it was sufficient for the purposes of this Study that they were only reported or noted by certain stakeholders (such as the media, NGOs, internal administration staff, etc.). A big challenge in identifying relevant cases was the lack of statistical information on corruption offences related to IT abuse and the fact that IT abuse for corruption seems not to be on the agenda of many, if not most, anti-corruption bodies in the region. At the same time, there seems to be a strong taboo against uncovering weaknesses in IT systems: it seemed as if public institutions were regularly very hesitant to reveal information that showed that their IT systems were much weaker than the public would perhaps believe. However, the initiators of this Study felt it was better to make case material available to an international readership, even if the material was not proven, complete, or representative, at least not in all instances.

The cases show that abuse of IT concerns the whole array of corruption offences:

- Bribery
- Abuse of office
- Trading in influence
- Conflicts of interest
- Procurement violations
- Embezzlement

Abuse of IT for corruption occurs in cases where financial interests are at stake, as well as in cases where the IT abuse serves only non-material interests of the public official (such as the satisfaction of publishing sensational private data). The cases seem to occur in every possible sector of public governance,

including state owned companies, and naturally on all levels of government (both central and local). Abuse of IT can occur spontaneously to cater to individual needs (such as a forged passport) or be part of continuous or organised crime schemes (such as Toll-system fraud).

The broad variety of cases also shows that the mantra "e-government helps in the fight against corruption" must be treated with caution. IT is not, *per se*, a panacea against corruption. In some cases, one could even argue that IT makes it easier for offenders to commit their corruption crimes: the opaqueness of IT systems can play to their advantage with traces being less visible in utterly complex networks and possibly ephemeral electronic records. The importance of sound safeguards (to be discussed in Chapter 2) becomes all the more obvious in light of these case studies.

Table 1

Title	Corruption offence (not necessarily proven)	IT use	Damage to public finances	How was the corruption offence detected?	Level of government (central or local)	Sector
Albania case 1: Corruption in the TIMS system of the border control	Bribery	Selling of forged data	Yes	Internal audit	Central	Law enforcement
Albania case 2: Corruption in the Electronic Public Procurement System	Procurement violations	Unauthorised entry/forgery	Yes	External audit	Central	Procurement
Albania case 3: IT corruption in the power distribution operator	Abuse of office Forgery	Forgery of data	Yes	Complaints by citizens	Central	Energy
Albania case 4: Embezzlement and forgery in bookkeeping	Abuse of office Embezzlement	Alteration of data/fraud	Yes	Internal audit	Central	Defence
Bosnia and Herzegovina case 1: The most famous Bosnian hacker amongs the prosecutors	Abuse of office	Computer sabotage	No	Internal investigation	Central	Judiciary

Title	Corruption offence (not necessarily proven)	IT use	Damage to public finances	How was the corruption offence detected?	Level of government (central or local)	Sector
Bosnia and Herzegovina case 2: Another controversial employment in Supreme Audit Institution of the Republic of Srpska	Abuse of office	Destroying of data	No	Insider information	Local	Procurement
Bosnia and Herzegovina case 3: Misuse of CIPS project's electronic system	Abuse of office	Falsifying data	No	Media report	Local	Civil registry
Croatia case 1: Call doctor for votes	Illegal obtaining of data	Unauthorised usage of patient data from hospital	No	Complaint by citizens	Local	Health
Croatia case 2: Confidential Croatian radio-television data base on the black market	Illegal obtaining of data	Copying and selling data from HRT database	No	Complaint by NGO	Central	Media
Croatia case 3: In search for veterans	Abuse of office Illegal obtaining of data	Selling or giving away data from the database	No	Media report	Central	Government
Croatia case 4: With a little help from civil servants, 68 Croatian passports were sold to criminals	Illegal obtaining of data	Checking confidential data from the police information system	No	Police	Central	Internal affairs
Croatia case 5: Policeman caught while inserting forged data into the police information system	Manipulation of existing data and procedures	Electronically creating fraudulent documentation to help foreign citizen to obtain Croatian citizenship	No	Police	Central	Internal affairs

Title	Corruption offence (not necessarily proven)	IT use	Damage to public finances	How was the corruption offence detected?	Level of government (central or local)	Sector
Croatia case 6: Policeman deleting traffic offences and disclosing confidential data (they accepted even roasted lamb and 20 litres of wine as a bribe!).	Illegal obtaining of data Manipulating data and procedures	Illegal obtaining of data: disclosing confidential data from the police information system to organised crime. Manipulation of existing data and procedures: deleting traffic offences from the police information system	No	Police	Local	Internal affairs
Croatia case 7: Accidentally caught for disclosure of confidential data on cars and their owners.	Illegal obtaining of data	Disclosing confidential data from the police information system to organised crime	No	Police	Local	Internal affairs
Croatia case 8: Every year 2 million euros disappears from the tollbooths	Embezzlement	Deleting data and inserting false data into the information system	Yes (≈2 million euros/ year)	Internal audit	Central	Traffic
Croatia case 9: Dirty cops; policemen disclosed confidential data to weapon smugglers	Disclosure of confidential information Abuse of office	Disclosing confidential data from the police information system to organised crime	No	Police	Local	Police
Croatia case 10: Policeman sentenced to one year in prison for allowing his friend to fish illegally	Disclosure of confidential information Abuse of office	Disclosing confidential data from the Ministry of the Interior information system to organised crime	No	Not known	Local	Police

Title	Corruption offence (not necessarily proven)	IT use	Damage to public finances	How was the corruption offence detected?	Level of government (central or local)	Sector
Croatia case 11: Senior inspector misused confidential data to win the local elections	Abuse of office Disclosure of confidential information	Illegal access to and disclosure of confidential data from the Tax Administration information system	No	Complaint by citizen	Local	Tax
Croatia case 12: You didn't spend a day of your life at work? No problem, you can still get a full pension!	Fraud (forging employment book) Embezzlement by awarding an unjustified pension	Inserting false data in Croatian Pensions Insurance Institute information system	Yes (≈20,000 euros)	Internal complaint	Central	Social security
Kosovo case 1: Destruction of Evidence	Abuse of office Fraud in office Falsifying official documents	Erasing data from the server	Yes	Complaint by citizen	Central	Construction
Kosovo case 2: Gaining the War Invalid status	Falsifying official documents Fraud in office	Falsifying data	Yes	Complaint by citizen	Central	Social affairs
Kosovo case 3: Misuse of the Password	Abuse of authorization	Favouritism Password theft	Yes	Internal complaint	Central	Health
Kosovo case 4: Falsifying of a tax document	Falsifying official documents Fraud in office	Falsifying documents	Yes	Internal complaint (former employee)	Local	Maintenance
Macedonia case 1: Abuse of the IT system on pay tolls	Abuse of office Bribery Embezzlement	False recording of number and type of vehicles in the pay toll IT system	Yes (≈2,000 euros)	Internal audit	Central	Transportation/ traffic
Macedonia case 2: Attack on the IT system for public procurement	Bribery Embezzlement Procurement violations	Hindering procurement process Illegal intrusion in computer system	No/not known	Complaint by citizen	Central	Procurement

Title	Corruption offence (not necessarily proven)	IT use	Damage to public finances	How was the corruption offence detected?	Level of government (central or local)	Sector
Macedonia case 3: Abuse of IT system and illegal disclosure of personal data	Embezzlement Abuse of office Possible bribery	Extracting personal data and creating an official document for another person	Not known	Detection of false document	Central	Administration
Macedonia case 4: Misuse of registering working hours system	Embezzlement Abuse of office	Altering data in working hours system	Yes	Internal audit	Central	Administration
Macedonia case 5: Abuse of administrator's rights (bank guarantees/ import quotas)	Embezzlement Abuse of office Bribery	Altering and re-altering data Opening and using fake account	Yes (≈160,000 euros)	Internal audit	Central	Border administration
Montenegro case 1: Abuse of office and forgery of official documents	Abuse of office	Falsifying data	No	Internal investigation	Central	Ministry of the Interior
Montenegro case 2: Using IT to inflict political damage	Manipulation and abuse of IT systems Abuse of office	IT system abuse Falsifying data	No	Media report (launched by offenders)	Central	Internal affairs Telecomm-unications
Montenegro case 3: Abuse of functions and entreing incorrect data in public registries	Abuse of office Bribery	Falsifying data	Yes	Internal investigation	Local	Land cadastre Internal affairs
Montenegro case 4: Illegal issuance of travel documents	Abuse of office	Falsifying data	No	Internal investigation	Central	Internal affairs
Serbia case 1: Sex at Belgrade Arena	Abuse of office	Illegal obtaining of data Manipulation of data and procedures	No	Media report	Central	Police

Title	Corruption offence (not necessarily proven)	IT use	Damage to public finances	How was the corruption offence detected?	Level of government (central or local)	Sector
Serbia case 2: When IT contractor "takes root"	Abuse of office Nepotism Procurement violations	IT contractor related risks Manipulation of data and procedures	Yes	Internal audit	Central	Justice
Serbia case 3: A senior public official spying on employees	Embezzlement Abuse of office	Illegal obtaining of data Manipulation of data and procedures	No	Whistle blower	Central	Economy
Serbia case 4: "Road mafia"	Abuse of functions Embezzlement Organised crime	Toll station systems were compromised by fake coprocessor emulator. Printing of double tickets with identical serial numbers for trucks. Raising of the entrance ramp illegally.	Yes	Whistle blower	Central	Transport-ation/traffic

Albania

By Edlira Nasi and Ened Kercini

Albania case 1: Corruption in the TIMS system of the border control

The case below concerns the abuse, by border police officers, of the border police office and the manipulation by them of the TIMS IT system (Total Information Management System), as a means to evade the payments due to the State for the use of an imported vehicle.

Background

Mr. A.I., through a special proxy, had given to Mr. E.H. the right to use a Ford vehicle, which had Italian car plates. Through this document, Mr. H. was given the legal right to appear and apply before the relevant institutions for the clearance procedures and registration of the car which had been imported and had, thus, to go through specific procedures in order to be used freely and legally in Albania.

However, E.H. had an acquaintance, Mr. A.T., an officer at the military base of Zall-Herr. It appears that E.H., the car owner, had confided to the officer that the car had been in Albania for quite some time, but was not accompanied by the proper documentation required to indicate its entry or import into the country, and he - as an owner - had not applied for said documents as there were quite a few financial obligations to be fulfilled in order to do so.

A.T. told E.H. that he knew a person who worked in Shkoder at the Murriqan Border Control Point, who could "fix" the car's documents in such a way as to appear that it had entered Albania only recently. Of course, for that service he would have to pay some money.

A.T. in turn was acquainted with Mr. A.S., who worked as a head in the Information Exchange Centre with Montenegro, at the Regional Directorate of Border and Migration, in the city of Shkoder. A.T. had promised E.H. that he could help to secure a document, according to which the vehicle had entered Albania during the last few days. In fact A.T. took it upon himself to complete this job, and, as a result, requested a photocopy of the real document evidencing the entry of the car into Albania, in order to produce

a new document from the Border Point, as if the car had entered Albania at a later stage (after 2009). A.T. is recorded to have said that the price had been 15,000 ALL (roughly 105 euros) in the past year, but that the price had since increased.

In order to secure the document and the help of A.S., E.H., A.S. and A.T. met on 9 February 2013 in a café in order to discuss the specifics. The next day, E.H. and A.S. met again to discuss the document of the entry point that was needed to be produced. A few days later, the two men met again, and A.S. said he completed his work and thus produced a report from the IT system TIMS[17].

False records in the IT system

The document produced falsely reported that the new owner of the car, E.H., had entered Albania from the Murriqan Border Point on 3 February 2013, at 05:58 along with a car with the plate number DK***L. This fact has also been documented by the records produced by the TIMS electronic system.

According to later reviews and audits of the TIMS system, it was shown that the person who had made the changes to the IT system TIMS was another man, Ad.S. During the discussions between E.H. and A.T., which were later recounted by E.H., A.T., the contact point, had told E.H. that he needn't even appear at the border point, as all actions necessary would be taken by A.S. who worked at the Border Point.

The way this was done was through accessing and falsifying electronic data in the TIMS system. The Total Information Management System (TIMS) is a large database which holds the data of all Albanians who have been issued a biometric passport, i.e. the majority of Albanians since the time biometric passports were adopted by Albania. The system records the movements of Albanian nationals that cross all Albanian border control points. Further to that, the system saves data regarding the means by which the citizens travelled, the point of origin and/or destination of citizens, as well as the vehicle registration numbers. The data is accessible also to law enforcement agencies and commissariats of the police. Given that as of 1 March 2012, biometric passports are the only travel document for Albanian citizens, all border control points use biometric passport readers and equipment for fingerprint verification. The real-time registration into the TIMS system of documents and their reading during entry/exit at border crossing points,

17 Court decision no. 1035, dated 23.07.2013

gives the possibility of comparison with the existing data thus reducing the possibility of abuse[18].

The intervention and activity on the TIMS system was performed by Ad.S. who had the task of the system operator at the Murriqan Border and Migration Police, as of the date 1 May 2010. In this position, he took part in the control of persons and vehicles, while he also registered them during the crossing at the entrance and exit to and from Albania. Ad.S. was also responsible and aware of the overall management of the border control TIMS system, and the system of cameras. His duties were also defined in the relevant regulation, which sets guidelines and standards of performance of duty for this position. In this position, he controlled and operated the TIMS sub-systems such as the system of border control and the criminal data system, while he also had the duty to supervise the work of other assisting staff during his shift, and to ensure that procedures were followed correctly.

The review of the system which took place as a part of the investigative process[19] showed that Ad.S. had made the change in the TIMS system, whereby it was indicated falsely that E.H. had entered Albania on 9 February 2013 as a way to avoid the payment of the relevant taxes or duties. This action is also proven by the TIMS report which indicates that the username of the person making these changes was that of Ad.S., as well as the fact that according to the schedule of work of the staff, Ad.S. was the operator of the system for that shift.

Due to these actions and the provision of money for said actions, the Prosecutor's office filed criminal charges against Ad.S., on the basis that he made false changes to the system and went against the public interest by making a false report regarding the vehicle of E.H.

A.S. was found guilty of passive corruption of public officials and sentenced to 1 year and 8 months of imprisonment (suspended sentencing under specific conditions) and he was banned from holding public functions for a year. Ad.S. was found guilty of abuse of office and sentenced to 6 months of imprisonment (suspended sentencing under specific conditions), and was banned from holding public functions for a year. A.T. was found guilty of exercising unlawful influence on public officials and sentenced to 6 months of imprisonment (suspended sentencing under specific conditions).

18 Information Exchange on the OSCE Code of Conduct on Politico-Military Aspects of Security - Republic of Albania 2013, FSC.EMI/178/14, 22 May 2014
19 The case was reviewed and pursued by the ICS through their informants, however the IT data appear to have been reviewed later as evidence by the prosecution

Albania case 2: Corruption in the Electronic Public Procurement System

The case concerns interventions in the public procurement system due to corruption, as well as an intervention in the electronic administration of public procurement.

Background

In fulfilling its role as the supreme independent audit institution in the country, the Supreme State Audit (SSA) conducted an audit of the Civil Aviation Authority (CAA) in 2012. The final report of the audit, "On the implementation of the legality and regularity of the economic-financial activity", of the CAA between the period 1 January 2011 to 31 March 2012 and the measures for the improvement of the process also included the review of procurement procedures[20].

The CAA is a public entity with financial independence, an aspect which allows the CAA to conduct its activity in accordance with international standards and in response to the need of the CAA to perform to high professional standards.

The administration of procurement procedures in Albania takes place in accordance with the law no. 9643 dated 20 November 2006 "On public procurement", law no. 9880 dated 25 February 2008 "On electronic signature", and the Decision of the Council of Ministers no. 659 dated 3 October 2007 "On the rules of the conduct of the procedures of public procurement by electronic means", as well as regulations and instructions of the Public Procurement Agency.

During one of said procurement procedures regarding the "Purchase of office equipment and furniture", the Supreme State Audit indicated irregularities in the procurement process while the answers of the officials involved indicated that there had been a manipulation of the electronic signatures in the procurement process.

20 Full report accessible at the SSA website http://www.klsh.org.al/web/pub/autoriteti_aviacionit_civil_394_1.pdf

The Procurement

During the above procurement process, communications within the contracting authority in the process (i.e. CAA), indicated to the SSA that, indeed, there were aspects of the electronic procurement that were irregular. On 20 October 2011, one of the staff members of the CAA, Mr. T., had been made aware of the signing of the minutes of a decision regarding the disqualification of a company in the above mentioned procurement process.

Mr. T. then informed the directors of the CAA that the commission who had evaluated the offers had never made said evaluation by electronic means, as he had been abroad. Moreover, he noted that the password he used as a user of the electronic system had been changed without him being notified and without his consent. Thus, someone else had completed the procedure of the review and the evaluation of the companies' offers.

Further to that, after reviewing the documentation of the offers that had been presented electronically (by using the changed passwords), Mr. T. had noted that the reasons for the disqualification of the company which had the lowest offer were not based on legal reasons nor provisions. As the company concerned had presented the exact same technical specifications as those requested by the CAA, the disqualification was unreasonable and would bring economic damage to the state budget and the CAA.

Mr. T. also confirmed that he had never taken part in this evaluation of the procurement offers, and neither had he taken part in a meeting on the same issue in 2011. From a verification made by the latter to the portal of the Public Procurement Agency, it was revealed that the evaluation was made by a third person after the change of a password. In a later document, as a member of the evaluation commission for the offers, he denied having signed the minutes of the meeting referring to that particular procurement process.

Despite these facts, the SSA notes that the directors of the CAA had not acted to rectify the condition by taking administrative measures for the persons concerned. As a result, the SSA sent the case to the Prosecutor's office noting that the actions of the CAA regarding procurements were fictitious since the members of the evaluation group for the offers denied having taken part in the evaluation of the offers.

Albania case 3: IT corruption in the power distribution operator

Background

In 2009, Albania went through the privatisation of 76% of the shares of the Operator of the Distribution of Electricity, whereby 24% of the shares of the Operator were owned by the Albanian State, and 76% of the shares were sold to the private company "CEZ Distribution". The distribution operator's activity was regulated by the Albanian Energy Regulatory Entity – ERE.

On 20 January 2011, the Office of Consumer Protection submitted to the Prosecutor's Office of Tirana a complaint against company executives of "CEZ Distribution" for the offenses of "fraud" and "computer fraud" referred to in Articles 143 and 143/b of the Criminal Code. The complaint, along with another complaint filed earlier by the police, stated that the company "CEZ Distribution" issued energy bills to customers that held a separate questionable item. Under the heading "Energy unaccounted for", there was an increased charging by 4,000 kilowatts for household clients, while for non-household consumers there was an added 20,000 kilowatts charge. The "energy unaccounted for" line item referred mainly to clients who illegally connected to the energy distribution network without registering or paying the relevant fees or to clients tampering with the appliances measuring the energy consumed. However, in most cases, clients complained that their bills did not inform them that the large amounts charged were a result of such a fine rather than a result of increased consumption.

Through its announcement on 12 January 2011, the Energy Regulatory Entity (ERE) informed the public, in its decision no. 90, dated 15 November 2010, that it had concluded that the practice of the application of "Energy unaccounted for" is improper and arbitrary. It is unsupported by law and contrary to the regulatory framework in place, and that for these actions "CEZ Distribution" was to be fined. In support of this, ERE had also received about 14,000 complaints from several citizens[21] in the time span of October 2010 to January 2011, out of which 490 fines had already been paid for by citizens.

According to the media, at the time (2011), the distribution operator had not only overcharged clients, but had done so in an abusive manner by allowing the inspectors to fine citizens and businesses without adhering to the procedures specified by the distribution company. Furthermore,

21 Tirana Court Decision no. 1633, dated 30 June 2014

the media alleged that the distribution operator's staff were incentivised and rewarded financially for fining clients,[22] thus leading to many clients being overbilled[23]. This, however, is not substantiated in the court minutes or decisions, despite the fact that no other reasoning is given for the said actions by staff members of the distributing company.

The total amount of financial damage to their clients during the aforementioned period was estimated to have reached 4-5 million euros[24].

The scheme of overbilling

The specifics of each billing of a client are done through operators in the field operating PDAs (Personal Digital Assistants). PDAs are devices used by company staff at the time of reviewing the energy consumption measuring appliances. PDAs transmit instantly (online) to the server the booth number, the number of the subscriber's contract, the position of the measuring appliance at that moment (i.e. registration of the amount of kilowatts consumed), and the date and time at which the measurement takes place. At that time, data on "anomalies" (i.e. technical issues, or illegal connection to the energy network, etc.) are also registered during the normal billing process.

The PDA readings are then synchronised with the MYAvis system running on the server in the Data Centre Server Room (technology data transmission is achieved through a GPRS platform) at the end of each working day. The data from the respective interface MYAvis pass directly through the billing system, except for information blocked according to specific filters, such as anomalies or suspicious billings, which are further reviewed.

During the time that one of the cases was adjudicated by the court, testimonies indicated that it was in fact impossible for employees to electronically alter client data, as they did not have administrator rights in the system. That led the prosecution to review the details of several measurements conducted by specific distribution company employees against whom there had been complaints. From the list of measurements of energy consumed, which also

22 Skandal/CEZ faturon me shume energji sesa blen, ve gjoba fiktive per te kerkuar rritje cmimi" dated 30.11.2011. Available at: http://www.gazetatema.net/web/2011/11/30/skandali-cez-faturon-me-shume-energji-sesa-blen-ve-gjoba-fiktive-per-te-kerkuar-rritje-cmimi/

23 "Hetimi, CEZ shperblente punonjesit qe mbifaturonin" http://time.ikub.al/2afad09e2d/445564cf92c2c0259d0562e9238b8515/Lajm_Hetimi-CEZ-shperblente-punonjesit-qe-mbifaturonin-abonentet.aspx

24 "Prokurorët, hetim 14 mijë ankesave për mbifaturim energjie" dated 27.11.2011 – available at http://www.shqiptarja.com/lajme/2706/prokuroret-hetim-14-mije-ankesave-per-mbifaturim-energjie-65833.html

indicated the place and time at which the staff of the company made the measurements, it was found that there were measurements conducted at unusual times of the day, such as at 22:00, 23:00, 24:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00 etc., despite the fact that the staff had already stated that the working time for measurements was between 08:00-16:30 hrs.

Additionally, the company distributing energy had already approved specific procedures for measuring the consumption of energy, which among others specified the complete rules and procedures to regulate the power measurement control system and method for calculating the energy consumed and other fines due to violations in the metering and illegal connections to the distribution network. This regulation clearly establishes that the measurement and fine had to take place in the presence of the customer or his relatives (photos, videos, and any other fact which confirms intervention in the meter). In the absence of the customer or his relatives or denial to sign the minutes of the measurement, the minutes have to be signed by the staff of another unit of the company (NTL unit). From the minutes of the measurements taken it was clear that neither the customers, nor staff of the NTL unit, had signed the minutes at the time that the excessive billings or fines for illegal connections to the energy distribution network took place. Indicatively, on 21 October 2010 alone, fines for about 17 illegal reconnections to the electricity network were recorded, all of them within 2 minute intervals of each other, or even simultaneously[25].

More than 10 people are suspected of taking part in this overbilling scheme. Further overbilling energy schemes have been discovered after this case and prosecuted. The court has already found guilty several staff members of the company and sentenced them, while cases for other staff members are still pending. Although in the case mentioned above, overbilling took place through PDAs, in other cases there are allegations also over electronic data having been altered, after they had been registered by the PDAs[26].

25 Tirana Court Decision no. 1633, dated 30.06.2014
26 "Prokuroria: Skema si CEZ vidhte 15 mijë konsumatorë" dated 15.04.2013 Available at: http://gazeta-shqip.com/lajme/2013/04/15/prokuroria-skema-si-cez-vidhte-15-mije-konsumatore/

Albania case 4: Embezzlement and forgery in bookkeeping

The case concerns an employee responsible for bookkeeping who, throughout many years, embezzled money administered by her and deposited it in her own bank account.

The defendant, Ms. M.K. was the head of finance of the Commando Regiment of Zall-Herr in Tirana. In this position, M.K. conducted actions contrary to the law, by appropriating funds to her own bank account that did not belong to her, through forgery of documents and other data.

In 2009, the Internal Audit Department of the Ministry of Defence conducted the "Thematic audit on the implementation of the legislation in force for dealing with salary and allowances of employees in the Commando Regiment Zall-Herr". The audit found that M.K., in her position as a chief of finance, had forged documents, namely the payroll of the employees of the Military Department no. 1200[27].

From the forensic accounting investigation, it was revealed that M.K had embezzled in total 8,668,886 ALL (61.920 euros), of which 6,198,326 ALL was as a result of net wage increases, and the rest of the 2,470,560 ALL through salary additions, per diems, services, etc. All of the funds came from the state budget and fund designated specifically for the military unit no. 1200 of Zall Herr Tirana.

The way the work had been organised at the office had been such that the finance specialist of the office only performed duties prescribed by the chief of finance, namely the concrete laying and preparation of the payroll lists. However, the specialist of finance did not oversee the summary of the payroll and the net wages of employees, as these payroll items were compiled by the Chief of Finance, namely M.K.

After the payroll lists were prepared, they would be handed over through email/electronic means, and the payroll would be approved by both the Chief of Staff and by the Commander of the Regiment. The means through which she managed to forge the payroll and receive the approval of the Chief of Staff and the Commander was by receiving the approval in writing (physical copy) before then altering the electronic data destined for both payroll and the bank.

27 Based on Tirana District Court Decision no. 41 dated 20.01.2012

The bank holds no responsibility for the wage discrepancies given that the bank was unable to control the data or have an overview of the wages, even if the amounts transferred to M.K.'s account appeared to be larger than what one would consider reasonable for a wage payment. After receiving the amounts in her account, M.K. withdrew them from the account and hid the money in other ways.

M.K. was found guilty by the court and sentenced to one year of imprisonment[28].

Bosnia and Herzegovina

By Aleksandra Martinovic and Srdjan Nogo

Bosnia and Herzegovina case 1: Hacking the email of the General Prosecutor

All relevant domestic and international reports about the judicial system in Bosnia and Herzegovina (BiH), including annual progress reports of the European Commission, are pointing out that the judiciary is dominated, controlled, and influenced by political elites, with constant political attempts to enhance the influence on appointments of judges and prosecutors throughout the BiH judiciary. The complex and dubious nature of BiH's judicial system and its shortcomings in relation to independence and impartiality can be described by the case of one State prosecutor (hereinafter Mr. X), who was accused of hacking the email of former General Prosecutor (hereinafter Mr. Y) in order to discredit him immediately prior to Mr Y's suspension from his official duty as a General prosecutor.

A possible motive of Mr. X for abusing Mr. Y's email can be found in his statement after the suspension of Mr. Y, where he is recorded stating that he would apply for position of the General Prosecutor of Bosnia and Herzegovina. There were also rumours that Mr. X was protecting some defendants whom Mr. Y had prosecuted.

Both Mr. X and Mr. Y were allegedly connected to certain political parties in BiH. Namely, Mr. Y was allegedly connected to the Party of Independent Social Democrats - SNSD - which is the leading party in the Republic of Srpska and one of the most influential parties in BiH, while Mr. X was at that time allegedly connected to the Social-Democrat Party (SDP) BiH, (the strongest party in the Federation of BiH), but also to the Union for a Better Future of BiH.

28 Ibid.

It was confirmed during the following investigation that Mr. X logged on to Mr. Y's email and sent false "General Instructions" to the employees of the Prosecutor's office of BiH and several media outlets from the Federation of BiH. The "General Instructions", containing compromising statements, was sent on 29 June 2011, on the letterhead of the Prosecutor's Office of BiH with a falsified signature of General Prosecutor.

These "General Instructions" stated that it was strictly forbidden for all employees of the Prosecutor's Office of BiH to give any comments on negative media articles about the General Prosecutor, particularly about articles on the then ongoing public affairs "Prisluskivanje" (Wiretapping), "Reket" (Racketeering) others, in which the General Prosecutor was allegedly involved at that time.

The "Instructions" also prohibited employees to read the magazines "Slobodna Bosna", "Dani", "Oslobodjenje", "Avaz", and "San", all published in the Federation of BiH, or to watch any programmes aired by the Federal television (one of the three public broadcasters in BiH), particularly the TV programme "60 minutes", broadcasted on that station.

The "General Instructions" also stated that *"prosecutors who think that we will start to hold regular monthly meetings, within the meaning of Article 20, paragraph 2, of the Rule Book, are 'fools'."*

After finding out about this email, General Prosecutor filed a complaint against an unknown person to the Court of BiH and the Prosecutor's Office of BiH, after which an order was given to the Federal police (within the Ministry of the Interior of the Federation of BiH) to start an investigation.

During the investigation, the inspector leading the fight against cyber-crime in the Federal Ministry of the Interior determined that the email of the General Prosecutor had been abused using a mobile phone (iPhone 4) registered to Mr X's mother, but exclusively used by him. Supposedly, Mr. X somehow got possession of a password for General Prosecutor's email and then used it to log in to it from a remote location and send the instructions. Despite the fact that most of the relevant security safeguards were in place in order to prevent this malpractice, it appears that the human factor was decisive in this case. After finishing the investigation, a report containing criminal charges against prosecutor Mr. X alleging the abuse of public office, forgery and fraud was sent back to the competent prosecutor's office (i.e. Prosecutor's office of BiH – Department for Organised Crime and Corruption).

According to some media sources, despite significant efforts of Mr. X's colleagues in the Prosecutor's Office to cover up this unprecedented scandal, the Office of the Disciplinary Council within the High Judicial and Prosecutorial Council (HJCP) of BiH was informed about the case.

But that was not the only charge against state prosecutor Mr. X. He was also accused of having committed two more disciplinary offences. Namely, he ordered the destruction of records relating to the examination of witnesses, in the presence of the same witnesses; and had sent a request for information to the Director of the Federal Police Administration, with content that was inappropriate for official correspondence, and the function that Mr. X was performing at that time. Namely, Mr. X requested, in a very inappropriate way, that the Director reveal a source of information and review an official police note which charged Mr. X, high officials of the Government of Federation of BiH, and of the Social-democratic party BiH for organising a conspiracy against the Director of the Federal Police Administration.

More than a year later, on 26 September 2012, the Office of the Disciplinary Council of HJPC BiH came to a joint agreement with Mr. X on the determination of disciplinary responsibility and disciplinary action. He thereby acknowledged and accepted responsibility for disciplinary violations, and the Office of Disciplinary Counsel withdrew the claim to determine his disciplinary liability for certain items from the disciplinary complaint.

When recommending the disciplinary measure, the Office of Disciplinary Counsel had in mind that *"the defendant had a successful career as public prosecutor and that he was engaged in complex cases which require high level of expertise and dedication"*. The fact that he was a family man and father of a young child, and the fact that he was burdened by debt were taken into account as mitigating circumstances. The fact that there was one more on-going preliminary investigation against him for charges of taking bribes was not even considered.

The First Instance Disciplinary Committee of Prosecutors of the HJCP, accepted the agreement between Mr. X and the Office of Disciplinary Counsel, and decided that Mr. X was responsible for three disciplinary offenses and a violation of the Code of Prosecutorial Ethics. It was considered a serious violation of official duty which called into question the public's confidence in the credibility of the Prosecutor's Office and harmed the reputation of the Prosecutor's Office of BiH. He was fined, with a deduction of his salary by 10 per cent for a six month period.

Only one day after his email was hacked, Mr. Y, the General prosecutor at that time, was suspended from his official duty because of his "inappropriate contacts" with international weapons smugglers. There had been numerous official records (photos and audio recordings) of his meetings and phone conversations with a weapon dealer blacklisted by the UN, indicating that Mr. Y was getting money and expensive gifts for helping a criminal network. In the end, corruption was not proven. Mr. Y stated that he regretted that his inappropriate meetings had harmed the reputation of the Prosecutor's Office of BiH, and he also made an agreement with the HJCP so that he was moved to a lower position – he continued to work as prosecutor for war crimes in the Prosecutor's Office of BiH, and his disciplinary fine was a 10 per cent reduction in salary for three months duration.

Bosnia and Herzegovina case 2: Another possible controversial employment in the Supreme Audit Institution of the Republic of Srpska

The Supreme Audit Institution of the Republic of Srpska (SAI RS) published a vacancy for the permanent employment of "two **junior** performance auditors". The vacancy was published in the Official Gazette of the Republic of Srpska on 3 May 2014, on the institution's website (on 29 April 2014) and in the media. The deadline for application was 30 days after this publication.

During that period, a total of 61 candidates applied for these positions and those who fulfilled the requested general and specific criteria and provided all required evidences and relevant documentation were invited to undergo a written test.

The test was conducted on 18 June 2014, in the IT cabinet of the Faculty of Economics in Banja Luka, and it was performed electronically by using computers in those premises.

As per the previous experiences for conducting similar tests, the work of all candidates was supposed to be printed out just after the test, copied on a USB device that belongs to the SAI RS, and deleted from the memory of computers in the Faculty of Economics. Also, each candidate who had taken the test normally had the right to make a copy of it to his or her USB memory stick.

But this time something went wrong. Although there is no official confirmation of this, allegedly, some data is missing due to problems in the IT system of the Faculty of Economics. There are several speculations within the SAI RS that either the complete test materials were not printed out, or that not all of them were properly recorded so that some data is missing, or even that there was nothing wrong with the technology, but that they are kept secret by the management of SAI RS (including members of the commission responsible for selection procedure), as an excuse for the disputable selection of one candidate.

In any case, there were no proper security measures in place and their absence allowed for this act. For example, instead of working in some safe software, candidates wrote their tests in simple word format without any protection, so that any person from the responsible commission had the opportunity to make changes to the tests. Furthermore, this time candidates were not allowed to make copies of the tests to their USB memory sticks and the tests were not given to them for review.

Despite the fact that no test results were published, shortlisted candidates were invited for an interview on 25 and 26 June 2014, and, according to the information published on the SAI RS website, *"the Commission responsible for the selection procedure determined the list of successful candidates and submitted it to the Auditor-General"*. Based on the proposed list, which has as yet not been made public, the Auditor-General had chosen two candidates.

While the first selected candidate seems to have been uncontroversial, there are already writings in the media about the controversy related to the selection of the second candidate. The case was detected because of the suspicion of other candidates (raised by the lack of transparency in the procedures outlined above). Therefore, some of the candidates filed complaints to the SAI RS.

As for the security measures to prevent these kinds of problems in the future, according to sources within the SAI nothing yet has been done. In addition to the fact that the selected candidate has a record of endangering public peace and order, his selection for the position of junior performance auditor at the age of 48 is rather questionable. The requirements for that position included only one year of necessary previous professional experience, and it was not explicitly stated that the experience was needed in the audit sector. At his age, the selected candidate is probably overqualified and could be selected for some other senior position.

According to some speculation in the media, he was brought to that position by a certain political party, which could make him susceptible to blackmail from the very beginning of his new public post. If some evidence appears to

substantiate these allegations, it is to be expected that he will be asked to do various counter-favours in return – to protect the interest of political elites and keep the information and evidence on corrupt practices in public institutions, which are subject to public audits, from being uncovered and prosecuted.
To add to the story of controversial appointments and employments in SAI RS during the past couple of years, the case of the appointment of the new Auditor-General is worth mentioning. Namely, the first choice of the RS Parliamentary Committee in charge of the selection of candidates was a person who was suspected of having obtained a false diploma. Due to strong pressure from the media, he was not appointed.

Bosnia and Herzegovina case 3: Misuse of CIPS project's electronic system

The Citizen Identification Protection System (CIPS) project started in Bosnia and Herzegovina in April 2002, when, on a temporary basis, a directorate for its implementation was established. The main task of the project was to establish a part of the system through which the Law on Central Registers and Data Exchange would be implemented.

In 2008, pursuant to the strategy for the development of identification documents, the Directorate became the Agency for Identification Documents, Registers, and Data Exchange (IDDEEA) of BiH. This institution follows, coordinates and institutionally governs the field of identification documents, pursuing relevant standards and regulations of the European Union and developing in accordance with such standards. It is responsible for personalisation and technical processing of the following identification documents: identity cards; identity cards for foreigners; driving licenses; travel documents; documents for registration of vehicles and other identification documents with the consent of the competent authorities and special Decision of the Council of Ministers.

From the very early stages of the CIPS project, a number of complaints were recorded about the misuse of its electronic system, particularly when issuing personal identity cards and passports throughout the country.

The Prosecutor's Office of BiH ordered a comprehensive investigation which was conducted in joint efforts with several institutions in BiH: the State investigation and Protection Agency (SIPA), several responsible ministries of the interior and police administrations, and the European Union Police Mission (EUPM) in BiH.

The first large operation was conducted on 28 May 2008, when 20 persons from several towns in BiH were arrested. This was followed by several more arrests during 2009. The arrested persons were mostly public office holders, such as police officers, employees of municipal administrations, and registrars, but there were also persons who were not public officials. Several of those in public office were suspected of being part of organised crime through misuse of their financial and technical resources, enabling the whole organised group to illegally obtain material gain.

First in the chain were police employees, responsible for the issuing of personal documents. They had access to a register of central evidence which is a part of the Agency system where data on all citizens of BiH are stored. Police officers used their official computers and authorities to entre the system and change data. Mostly, they would find a person in the database who had BiH citizenship yet had never received a personal ID card (for example, if the person went abroad during the war and never came back). They then sent the person who wished to receive a false document to a registrar's office (another part of the organised criminal group operating within the jurisdiction of the municipal administration) where they would provide a birth certificate and a certificate of citizenship in a false name, which was enough to start the procedure for obtaining the personal ID card. Even the data of dead persons was used; rather than officially registering the death, they registered the person as having lost an existing, valid ID card and started the procedure for the issuance of a new ID card.

As stated by the Prosecutor's Office of BiH, *"the suspects were charged for having misused the system for personal documents in BiH in a way that they enabled citizens of BiH and other countries in the region issuing of original identity documents of BiH, which contained false information about the identity of the persons or their nationality"*.

The investigation produced evidence that illegally obtained personal documents were used to a considerable extent for criminal activities in various parts of the country and the region. For example, there were suspects that had been members of the Zemun clan, suspected for the murder of former Serbian Prime-Minister Zoran inđić, and the attempted murder of Serbian politician Vuk Drašković, as well as several other members of the criminal underground who obtained false BiH identity documents.

There were also suspicions that arrested persons were selling original identity cards and passports of BiH with false identities for 2,000 euros. More than 200 invalid ID cards and passports were issued in Banja Luka alone.

This huge case caused a great deal of damage to the reputation of the public service in the whole country. As a result, a number of changes in procedures were initiated in order to prevent similar cases arising in the future. For example, procedures within the registrar's offices were significantly reinforced so that it is no longer possible to get a birth certificate and a certificate of citizenship for a third person without said person's authorisation. There are also additional electronic checks in the registrar's offices, ministries of the interior and other competent administrative bodies for determining the identity, stay and other relevant data of persons when issuing their personal documents.

Croatia

By Zorislav Petrovic and Ivana Andrijasevic

Croatia case 1: Call doctor for votes

During a campaign for local elections in May 2013, citizens of Dubrovnik with diabetes received a letter from a diabetologist at the Dubrovnik General hospital, who was running for mayor. Many of his patients got a personal letter from him, in which he reminds them of his candidacy, while stressing that he is ready to help them: *"(…) my first choice is to be at your service, my dear patients"*. He also reminded his patients of the huge progress that had been made with the creation of the most modern centre for diabetes and mentioned *"this year we are celebrating 20 years of Diabetes Society"*. When one activist group discovered this, it immediately demanded an investigation from the Municipal State Attorney's Office (DORH) in Dubrovnik.

An investigation was started right away and revealed that the call centre of HNS (Hrvatska Narodna Stranka – Croatian People's Party), which he was a member of, called in total 3.133 fixed phone numbers in the Dubrovnik-Neretva County, and that 3.215 (98%) were numbers of his patients. All of those numbers, together with the names and addresses, were filed in their personal files in the clinic for Diabetes and Endocrinology, where he worked as a doctor. For DORH in Dubrovnik, such a high percentage *"provided an indication that the patients' registry containing their personal data was used for the electoral campaign of the diabetologist"*. However, he denied that he had ever asked anyone to get him such data for the electoral campaign.

During the investigation, DORH discovered that numerous persons in the general hospital in Dubrovnik had access to the list of patients and their personal data. Furthermore, DORH discovered that the list used in HNS's call centre was set up

by more than one person and that several different sources were used. Therefore *"it was not possible to establish where and from whom those data bases were obtained"* and therefore, there was no basis for further prosecution of the mayoral candidate.

During the investigation, he claimed that he was using public data for sending letters, and that he could only acquire data for his own patients, but not for patients of other doctors. Still, another doctor in the same clinic where the diabetologist in question worked, confirmed that anyone with basic system knowledge could access complete patient records. She claimed that he himself got her the data of all patients for a study she was doing. The administrator confirmed that a majority of nurses and doctors are authorised to access that data. The administrator also confirmed that he got the data for the other doctor and one nurse upon their demand for "some anniversary".

As a result of DORH's decision not to prosecute the mayoral candidate, on 5 March 2014, a club of City counsellors "Srđ je naš" informed the Croatian Association for the Promotion of Patients Rights about this case of patient data abuse. The aim of this communication was to ask the association to use its influence and back up the counsellors' demand to DORH to delegate this case to State Attorney's Office outside the city of Dubrovnik.

Just a few days later, on 7 March 2014, associations gathered in "Platforma 112" to file charges against the Municipal State Attorney's Office in Dubrovnik due to suspicion of political corruption. One specific accusation claimed that, despite evidence, this institution incorrectly dismissed the allegations against the diabetologist. They also informed the Croatian People's Ombudsman about the lack of investigation from the Croatian Personal Data Protection Agency on this issue, and criticised the Croatian Medical Chamber.

There are at least three possible scenarios of IT misuse in this case:

a) private data of patients was obtained illegally by someone in the Dubrovnik general hospital, presumably close to the mayoral candidate, for the sole purpose of creating a mailing list for the local elections;
b) somebody broke into the database from the outside – it was hacked, and nobody from the hospital would be directly responsible for that;
c) somebody from the hospital got the data for a different purpose and then someone close to the mayoral candidate got hold of the data, too.

Croatia case 2: Confidential Croatian radio-television database on the black market

According to the Croatian Radio-Television Act, every physical and legal person in Croatia who owns a TV or radio set is obliged to pay a licence fee. HRT holds and administrates a register of HRT monthly licence payers in the Republic of Croatia. This register is not publicly available. Since it contains users personal data, such as name and surname, address, Personal Identification Number (OIB), etc., its management and usage are protected by provisions of personal data safety legislation. According to the information from the publicly available Central Register with records on personal data filling systems in the Personal Data Protection Agency, the HRT register is on the server to which physical access is granted exclusively to authorised persons. Authorised users use data from the register by inserting their username and passwords or certificate. Application is available by the local network and internet, by using protected data tunnels. Finally, safety copies are in the server room.

However, in 2004 a CD containing a copy of this database appeared on the black market. Allegedly, the CD had been made by a Croatian Radio-Television (HRT) employee who works with this database and profits from its illegal selling.

In this case, IT has been misused for the purpose of intentionally copying and selling data by an employee of HRT who either had access to the register or who knew someone with access to the register. As a result, all the above mentioned technical safeguards have been breached, as well as provisions of the General rules on work and conduct of HRT, according to which employees of HRT need to work in accordance with the highest business standards and basic ethical standards, based on several values, including confidentiality and protection of data, in accordance with relevant legislation and general rules. Evidently, these standards have not been applied.

A member of the Management Board of the NGO "Potrošač" ("The Consumer"), reported this case to the Department of Economic Criminal Offences (DECO) of the Ministry of the Interior. Due to frequent complaints from Dalmatian subscribers who felt harassed by various companies that provide their services through catalogue offers using addresses from the HRT database, in 2004, HRT organised an internal investigation into the department for the collection of licensing fees. However, the investigation yielded no results and subscribers are still targets for various sensational offers by companies.

Croatia case 3: In search for veterans

For years, one of the biggest disputes in Croatian society has centred on trying to specify the exact number of war veterans. There has always been speculation that many more people were actually involved in the defence of the country during the War of Independence than has been recorded. Since official data on the issue was never published, it was one of the main topics in political fights between the ruling national-conservative HDZ (Hrvatska Demokratska Zajednica – Croatian Democratic Union) party and the opposition. HDZ was always reluctant to publish the veterans' register, and the opposition accused them of hiding the figures because it would enable a lot of people, who did not have an actual right, to use the privileges of veterans. Veterans are allowed numerous benefits, starting with high pensions, free apartments and privileges when buying a car. According to the opposition, HDZ was – in this way – buying popular support. On 6 April 2010 the website www.registarbranitelja.com suddenly published an incomplete list of veterans[29]. Authors of the site were anonymous and, as they wrote on the site, their goal was to stop corruption and to make Croatian authorities publish a complete list of the veterans.

This publication caused fierce reactions throughout the country. Then Prime Minister Jadranka Kosor called it a "deed of (the) intelligence underground", and the Interior Ministry immediately announced that it was a criminal act punishable by up to three years in prison. The Ministry of Defence (MoD) and the Veteran Ministry (VM) demanded immediate investigation from the State Attorney. DM also announced that its IT system was not endangered, and that it had not suffered any sort of attempted cyber attacks.

The Former Veteran's Minister claimed that many people had access to such data. He claimed that in 2003, when he was in office, that he received data on CDs. According to Pančić, the Government could find out when the data was stolen by simply comparing the published information with the actual register. *"When I was minister, there were 403,000 veterans, now there are more than 500,000...maybe somebody stole the CD six years ago and published it only today"*, said Pančić.

A couple of days later, the police found data with four former employees from the Office for Defence (a branch of the MoD) in Karlovac, and suspected them of stealing the data. The investigation showed that these four had indeed published data on the internet, but also that employees in

29 Veterans were involved in defence through the Ministry of Defence and Interior Ministry – this list contained only people involved through the Ministry of Defence.

the Office for Defence, in total 23, had access to the same data. No charges were pressed against the four from Karlovac. Further, there has been no other news in the media of anyone else being charged for the breach. The Croatian Government did demand the company hosting the website, www.registarbranitelja.com, take the information down, but the owner refused. The veteran register was online until April 2012, when the domain name expired. The official register was published on 19 December 2012, and included most of the data published on the unofficial website.

This is an example of abuse of office. Since the data was published we can assume that somebody from one Office for Defence took data, published or gave it, or even sold it, to someone else who then published it. There might be many different motives for publishing the register, starting from political disputes to noble motives, such as trying to increase transparency. Still, there is no doubt that the main reason why that happened was a lack of minimum security protocols involved in the procedure of dealing with the data distributed to the Offices for Defence in different Croatian cities.

Croatia case 4: With a little help from civil servants 68 Croatian passports were sold to criminals

In a joint action the Ministry of the Interior (hrv. Ministarstvo unutarnjih poslova – MUP) and the Bureau for Combating Corruption and Organised Crime (hrv. Ured za suzbijanje korupcije i organiziranog kriminaliteta - USKOK), under the code name "Border", identified seven persons accused of forgery and selling Croatian passports to criminals from Serbia, Bosnia and Herzegovina, and Montenegro. From 2006 until the end of 2010 the group sold 68 forged passports for 10,000 euros each, thus earning a minimum of 680,000 euros.

One civil servant in the Croatian Consular Office in Orašje in Bosnia and Herzegovina was not brought before the court as she made a deal with USKOK and accepted a penalty of one year in prison. Another, who worked as a senior officer in the Division for Passports of the Zagrebačka County Police Administration, was accused of abusing her powers and was sentenced to 13 months in prison. Five other members of this criminal organisation are still awaiting trial.

The role of the mastermind behind the entire operation was to get information about people who possess Croatian citizenship but have no passports. He would arrange forgery of passports with third parties (mainly

criminals), collect photos, and half of the agreed amount of money. The role of two policemen and one senior officer in the Division for Passport of the Zagrebačka County Police Administration was to check the accuracy of the data previously collected by their colleague about the people who possess Croatian citizenship, but have no passport. They checked for this data in the MUP information system, precisely in the register for travel documents of Croatian citizens (hrv. Evidencija putnih isprava hrvatskih državljana), which represents one of the registers within the MUP information system.

They could perform this task since both, in accordance with their working position, had the login and password needed to access the Register of travel documents of Croatian citizens. Although this database was to be used for professional use only, they have misused their powers and accessed the database for criminal use.

After obtaining all the necessary information about the people whose forged passports would be used, they then forged the authorisation for collecting the passports. With this authorisation, the passports could then be collected in the Diplomatic and Consular Missions of the Republic of Croatia in Bosnia and Herzegovina and Serbia. That part of job was assigned to a civil servant, who worked in Croatian Consular Office in Orašje, Bosnia and Herzegovina.

Croatia case 5: Policeman caught while inserting forged data in the police information system

In 2005, a policeman from Zagreb inserted false data in the official police records confirming that a 64 year old man from Serbia and Montenegro reported the loss of his Croatian ID card, despite neither possessing Croatian citizenship nor a Croatian ID card. Furthermore, he printed a confirmation letter on the loss of the ID card, certified it with an official stamp and inserted it into the MUP information system, precisely in the Register of ID cards (hrv. Evidencija osobnih iskaznica), which represents one of the registers within the MUP information system. He could perform this task since he, in accordance with his working position, had the login and password to access the Register of ID cards. By doing so, he abused his powers by entering forged data in the Register.

During the routine monitoring process, the head of the police station noticed this confirmation letter in the information system and became suspicious

about its authenticity. After a verification process it was determined that this confirmation letter was forged and that the policeman under suspicion had misused his powers. As a result, the policeman has been detained from service and the police pressed criminal charges against him.

According to information from the police, the suspected policeman did not receive a bribe from the citizen of Serbia and Montenegro. He forged the confirmation letter on the loss of ID as a favour to a joint friend to improve the legal position of the 64 year old who tried to obtain Croatian citizenship.

Croatia case 6: Policemen deleting traffic offences and disclosing confidential data: they even accepted roasted lamb and 20 litres of wine as a bribe!

After a long period of eavesdropping and following, a joint action by the Ministry of the Interior (MUP) and the Bureau for Combating Corruption and Organised Crime (USKOK), conducted under the codename "Kamion", concluded in the arrest of 37 persons, 11 of whom were policemen, under suspicion of disclosing confidential data from the MUP information system. The policemen were suspected of misuse of powers and receiving bribes from the owners of transport companies, craftsmen, and carriers. They were also suspected of disclosing information on the location and timing of control of transport vehicles by Croatian Motorways Ltd. (Hrvatske autoceste – HAC) on at least 80 occasions. HAC is one of four companies that operate the Croatian Motorways Network surveying transport of dangerous goods, by revealing data on vehicles from the MUP information system. Finally, they were suspected of deleting traffic offences in the MUP information system. The bribes received for the aforementioned service was money, and in one case a roasted lamb and 20 litres of wine. In accordance with their authorities and needs as traffic policemen they had login and passwords which allowed them to access various databases within the police information system, among others data on location and timing of controls of transport vehicles by Croatian Motorways Ltd. surveillance of dangerous goods transport, as well as data on vehicles. Although their primary role was to ensure the safety of all participants in traffic, they had decided to misuse their powers and accessed the database for criminal use.

Croatia case 7: Accidentally caught for disclosure of confidential data on cars and their owners!

While tracing the organisers of an international prostitution ring during a Croatian-Spanish police action with the codename "Catalunya", detectives accidentally discovered an offence by a traffic policeman and an administrative officer in the Međimurska County Police. Over a period of two months, the policeman and the administrative officer had disclosed confidential data on cars and their owners to one of the detainees arrested during action "Catalunya". The detainee, who is a former policeman, apart from recruiting girls to work in Lloret de Mar, Spain, where they had been forced into prostitution, was also in the car reselling business. When buying used cars, the traffic policeman and the administrative officer passed on data to the detainee on the car and its owner from the MUP information system, precisely from the Register of Registration of Motor Vehicles (hrv. Evidencija registracije cestovnih vozila). They could perform this task since they, in accordance with their working position, had the login and password to access this Register. By doing so, they abused their powers and have violated personal data protection laws.

It is not known if it was done for monetary gain or as a favour to a former colleague. Criminal charges were filed against both, and they were suspended from the police until the finalisation of the discipline procedure.

Croatia case 8: Every year 2 million euros disappears from the tollbooths

On 31 December 2013, the total length of the motorway network in Croatia amounted to 1,288.5 km. When using motorways, drivers are obliged to pay road tolls. The total revenues from the tolls in 2013 amounted to 296,688,044 euros (excluding VAT)[30]. However, according to some directors of Croatian Motorways Ltd. (Hrvatske autoceste - HAC, one of four companies that operate the Croatian Motorways Network), 1% of the tolls, worth 1.7 to 2 million euros, disappears every year. The main suspects for this loss are employees of the HAC who work in the tollbooths. HAC has noticed that some of their employees generate up to ten times the number of invoices which are then cancelled and re-printed with changed data. For

30 HUKA – Croatian Association of Toll Motorway Concessionaires. National Report on motorways in Croatia for the year 2013. Available at: http://www.huka.hr/en/news/223-national-report-on-motorways-in-croatia-for-the-year-2013

example, when a truck appeared at the tollbooth, the employee working in the tollbooth would ask the driver to pay the regular toll for a truck (which is higher than for cars). Then he would access the information system, cancel the just issued invoice, insert false data - that is to register that the vehicle passing was not a truck, but a car - and printed a new invoice. Since the toll was (and still is) higher for trucks than cars, he would keep the surplus of money for himself.

In August 2010, an internal audit control of Autocesta Rijeka Zagreb d.d., the second company that operates the Croatian Motorways Network, revealed that 22 employees were stealing money from tolls on Demerje and Lučko. They have been reported to the police and subsequently fired. Guided by the principle *in dubio pro reo*, the judge stated that the court suspects that they have misused their working place and committed a crime, but that there is no evidence to prove their crime. While reading the acquittal, the judge invited them to read E.A. Poe's poem 'The Raven', and pay special attention to the last sentence of every strophe: *Never again!*

In this case, Autocesta Rijeka Zagreb d.d. had used the internal IT systems auditing as a safeguard against IT corruption. As a follow-up to the judges' poetic acquittal in order to prevent similar cases in the future and as an IT safeguard measure, the management of HAC decided to install cameras monitoring the work of employees in tollbooths. These cameras will not capture faces of employees nor their voices, but only their working space, hands and the process of paying/collecting the toll. The total amount of this investment was 354,000 euros.

Croatia case 9: Dirty cops - policemen disclosed confidential data to weapon smugglers

Three policemen from Zagreb were accidentally caught disclosing confidential data from the Ministry of the Interior (MUP) information system to weapon smugglers. While eavesdropping on a conversation between weapon smugglers and the police, internal affairs police investigators heard of disclosure of confidential data from the MUP information system. Besides disclosing confidential data, the policemen had deleted criminal charges; forged documentation; and even given advice to some of the arrested criminals on how to defend themselves during the investigation and warned them in case they were followed by the police.

The first suspect revealed various pieces of information and data from the MUP information system to his friends, some of who were criminals. Information

revealed included issuing of arrest warrants, private information about a waitress they had hired in their coffee bar, or information about a nephew who ran away from home. The two other policemen helped their colleague obtain all of this information and data from the MUP information system.

They could perform this task since they, due to their working position, had the login and password details to access various registers. By doing so, they abused their powers and violated personal data protection laws.

Namely, "*secrecy, integrity, continuous availability and control of the data and information from the MUP information system usage, is implemented through a number of organisational, system and program measures and procedures as well as division of responsibility and authorisation. All users of the MUP information system are obliged to implement data protection, as prescribed by the Ordinance on the protection of MUP information system based on the electronic data processing, the Ordinance on safety and protection of MUP official data and other internal directives and instructions which operates activities on MUP information system data protection. Responsibilities of officers working position define the level of data accessibility*".

As a result of the investigation, police filed charges against 23 persons, among them 3 policemen. 13 of the accused pleaded guilty and settled with USKOK for lenient punishments. The first suspect was finally sentenced to 6 months in prison, a punishment that has now been replaced by 50 days of community work. The Court also prohibited him from working as a policeman for three years. The 2 other policemen, together with 8 persons accused of receiving illegal information from the 3 policemen, still await trial.

Croatia case 10: Policeman sentenced to one year in prison for allowing his friend to fish illegally

In May 2012, the Council of the County Court Rijeka convicted two former policemen and one other person for the abuse of confidential police data. The first former policeman had disclosed information from the Ministry of the Interior (MUP) information system on vehicle registrations and profiles of its owners to his acquaintance. To cover his entrance into the system and to acquire the information itself, he used the login credentials of his colleagues. By doing so, he had abused his powers and violated personal data protection laws.

Namely, "*secrecy, integrity, continuous availability and control of the data and information from the MUP information system usage, is implemented through*

a number of organisational, system and program measures and procedures as well as division of responsibility and authorisation. All users of the MUP information system are obliged to implement data protection, as prescribed by Ordinance on the protection of MUP information system based on the electronic data processing, Ordinance on safety and protection of MUP official data and other internal directives and instructions which operates activities on MUP information system data protection. Responsibilities of officers working position define the level of data accessibility".

He was sentenced to one year in prison for conducting three criminal deeds of misuse of power. He was further prohibited from working in the state administration for the next five years. Another former policeman was sentenced to 5 months in prison for encouraging the other to conduct criminal acts, while their acquaintance was sentenced to 4 months in prison for the same offence.

From December 2007 until June 2008, the first convicted policeman had also disclosed information from the MUP information system to his retired colleague. This information referred to the time when the police patrol boats were patrolling the Poreč sea surface. As a result, he knew when it was safe to illegally extract date-shells (lat. Lithophaga lithophaga, hrv. prstac), a shellfish which is strictly protected by the Ordinance on Designating Protection and Strictly Protected Wild Species (Official Gazette, no. 7/06 and 99/09).

Croatia case 11: Senior inspector misused confidential data to win the local elections

A senior inspector from the Tax Administration within the Ministry of Finance had accessed the information system of the tax administration in 2010, intending to find out the amount of tax debt owed by his rival at the elections for the president of the basic branch of the Croatian Democratic Party (HDZ) in a part of Zagreb called Španˇsko. Furthermore, he used data from the Register of Tax Payers showing his rival's tax debt in order to make a leaflet for the forthcoming elections, held on 1 June 2010. On this leaflet, separated from information about the tax debt, he wrote *"With those who evaded taxes to the state, we surely will prosper?"* He could perform this task since he had been authorised to access certain personal data of taxpayers including, among others, his rival. Finally, he won the elections.

Consequently, his rival filed charges against him for abuse of powers to the State Secretary of the Tax Administration. The Civil Servants Court found

him guilty of a *"serious breach of professional duty"* and penalised him by reducing 15 per cent of his salary for a period of 4 months. He submitted an appeal to the Higher Civil Servants Court, which was refused. On the basis of this decision, his rival filed charges against him to the Court of Honour of HDZ. However, the party was lenient and reproved him for his deeds.

According to article 62 of the Income Tax Act (Official Gazette 177/04, 73/08, 80/10, 114/11, 22/12, 144/12, Decision USRH-120/13, 125/13, 148/13) for the purpose of providing the data necessary for the tax assessment; taxpayers or their authorised representatives are obliged to submit an application for the enrolment in the register of income taxpayers to a local office of the Tax Administration responsible for their domicile or habitual residence.

Article 8 of the General Tax Act (147/08, 18/11, 78/12, 136/12, 73/13) introduces the concept of a tax secret. All data stated by the tax payer and all data obtained during taxation procedures are considered to be a tax secret. This represents a form of protection which prevents unauthorised usage or publishing of such data to the public. The obligation of keeping tax secrets applies to all official personnel, experts and other persons involved in taxation procedures. However, Article 8, paragraph 2, of the General Tax Act contains provisions that mean, under certain circumstances, some data will not be considered to be a tax secret. These are: data on the date of entry to and data on the date of exit from the value-added tax system, and data on tax payers who were providing false data regarding value added tax. Paragraphs 5, 6, 7 and 12 stipulate cases in which the obligation of keeping the tax secret will not be breached. Furthermore, according to the provisions of Article 9 of the General Tax Act, parties to tax law relations are obliged to act in good faith; that is conscientiously and fairly. In the particular case described above, the senior inspector of the Tax Administration within the Ministry of Finance misused his powers. Manipulating data from the Register of Tax Payers to discredit his political opponent breached the tax secret. His behaviour was not ethical nor in good faith.

Croatia case 12: You didn't spend a day of your life at work? No problem, you can still get a full pension!

Although she has never worked, in 2007 one elderly lady started to receive her pension. During the last three years, she received more than 20,000 euros. As of 2007 her daughter was working at the Croatian Pensions Insurance Institute (HZMO) as Head of the Internal Audit Office. Her

colleagues suspected that she accessed the pension information system and changed her mother's details to allow her to be a pension recipient. Accordingly, they reported this suspected fraud to the management of HZMO. She could do so as she had access to two registers of the HZMO: main register on persons using pension insurance (hrv. Matična evidencija o osiguranicima mirovinskog osiguranja) and main register on users of pension insurance rights (hrv. Matična evidencija o korisnicima prava iz mirovinskog osiguranja).

During the investigation, it was discovered that she had forged an employment book, so criminal charges were also filed against her. However, although the investigation proved that her mother had no right to receive a pension, the police could not prove that her daughter had helped her to obtain this right. Finally, she was transferred from the position as head of the Internal Audit Office to the position of coordinator in the Sector of Economic Affairs. Although her mother was not entitled to receive pension funds, she never returned the illegally gained pension.

Kosovo

By Hasan Preteni and Driart Elshani

Achievements in the field of Information Technology (IT) have helped greatly in the modernisation of national institutions, thus giving greater power to the work efficiency of institutions. However, not everything is in favour of genuine and effective work. Based on the Anti-corruption Agencies' working practices since 2006, Kosovo has had many cases where Information Technology was not used for its intended purpose.

Each civil servant in Kosovo has his/her own official e-mail which has the domain @rks-gov.net. This e-mail should only be used for official communication between officials and others - and only for official duties. Each user within this domain can easily find and write to email accounts of other state institutions employees. Around 70,000 employees in Kosovo institutions use the above mentioned e-mail domain. This number includes the central, regional and local government levels; officials of all "jurisdictions" (legislative, executive and judicial); the Office of the President; and other independent mechanisms such as: the Kosovo Police and different agencies established by the Assembly of Kosovo or through other mechanisms.

Official email addresses should be used only for official communication. However, often there are cases when the network is used for private-personal issues or for political party or commercial purposes. People of influence, during the election campaigns, often misuse the official e-mail by invoking civil servants to vote for them or for their political party.

Some of the civil servants in cooperation with various businesses have established alleged "Professional organisations for Civil Servants training", where training budgets have been embezzled. Furthermore, Kosovo's institutional computer network has been misused, by sending different advertisements which invite the institutions (civil servants) to travel abroad on seminar trips paid by the institutions. This has caused officials to attend unprofessional training sessions with poor organisation which were not viable for the institution but very profitable for the companies that organised the training in cooperation with the IT officials.

A flagrant violation was recorded on one occasion when a director of a department in one of the ministries opened a restaurant outside the capital Prishtina, and through the @rks-ks.net e-mail advertised its opening, and used the official e-mail to send out invitations, even to central institutions leaders, to participate in the opening ceremony. This advertisement proved to be harmful for the civil servant, since a few days after the media discovered that the civil servant used the official e-mail to advertise and send the private invitation, his restaurant was attacked and burned to the ground never to be opened again. However, this might have been due to public outrage because he opened a restaurant as a public official, rather than the chosen means of communication.

All Kosovo institutions have their official web sites on the Internet. However, as a result of the institutions' insufficient computer network security, almost all institutions have at least once been attacked by "hackers".

Cases when civil servants, during working hours, use their computer to communicate with different persons on their social networks, thus not being efficient in their work and misusing institutional technology for personal needs, are not rare.

Several cases when officials use the internet, after working hours, to watch pornographic material or surf various networks that propagate immorality have also been identified.

In addition to these forms of unwanted use of information technology, below will be presented some specific cases which damaged the institutions and benefited individuals.

Kosovo case 1: Destruction of Evidence

In post-war Kosovo, many demands appeared to stabilise the situation and provide immediate welfare for citizens by creating new jobs and establishing the conditions for overall development of the country. One of the priorities of the Government at that time was to improve the road infrastructure. A considerable amount of funds were allocated for paving both local and regional roads. Due to the post-conflict situation, very few companies specialised in this type of work. Citizens' expectations were great, therefore, any action was welcomed by the citizens. However, the public soon realised that the road restoration work was not being done to the same standard as was the case before the war.

Some of the central government officials misused this situation. Officials, in cooperation with the owners of the construction companies, started to misuse the funds and to disobey the law in force. State officials started asking for bribes from each company who wished to receive contract work.

The amount requested for contracting a job was between 10-20% of the total value of the tender. Since its establishment, the Anti-Corruption Agency has received information about numerous allegations of corruption in this field. The most specific case was when a business owner complained that in order to contract a job worth millions, state officials had requested a high, seven-digit payment (or 15%) of the total value of the tender.

This businessman was very concerned and decided to contact the Anti-corruption Agency. He was received by Agency officials, and considering the Agency's mandate and the signed Memorandum of Cooperation with the prosecutors of the European Rule of Law Mission in Kosovo (EULEX), the Agency decided to forward this information to EULEX. The value of the tender was very high, and so was the level of the persons suspected of having requested a bribe. The case was very sensitive, and the investigations commenced immediately. In mid-2007, investigators intervened on the premises where these officials operated, controlled the premises and obtained a great deal of physical material, some computers and other electronic material, and some of the officials were arrested.

A few days later, Agency officials seized some other electronic equipment located in the Ministry of Public Administration. According to the institutional rules applied to all public administrations in Kosovo, the servers for storing the data of all government institutions are located within this ministry. On that very same day, EULEX investigators also arrested two IT officials. The findings were that the entire material which the investigators expected to find

on the Ministry's servers and which would prove the suspicions of the Anti-corruption Agency concerning irregularities and violations of the law, were deleted from the government servers. The sole purpose of these investigators was to enable the provision of evidence against the officials involved in corruption. It was therefore the assumption that data containing evidence of other companies' bids with lower prices were deleted. By deleting such data from the server, the goal was to give the tender to the most expensive company. The investigations continued for several years, and now the case is having its epilogue in court. The list of persons charged, in addition to the officials from the road department, also includes the two IT officials from the Ministry of Public Administration who obstructed investigations by deleting the data from the main servers. The overall number of officials charged is 8-10 persons. The criminal offences that they are charged with are misuse of official duty, fraud in office and falsification of official documents. As a measure to prevent further similar cases, servers could be put under some form of independent control.

Kosovo case 2: Obtaining the status of "War Invalid"

A special department for war invalids exists within the Ministry of Labour and Social Welfare. In June 1999, after the war in Kosovo, many persons applied for enrolment in the war veteran list. Later, in 2003-2004, the work on treating the war veterans list commenced. There were many applicants, and it was very tempting to register people in the list, as in addition to material benefits, they would gain other benefits such as: preferential medical treatment; purchase of vehicles without paying the custom duty; and other privileges and benefits for themselves and their family members. Some of them immediately gained the status, whereas some gained the status later on - those who gained the status later presented a problem.

A person informed and denounced to the Anti-corruption Agency another person with the initials F.M., who was enjoying a war invalid pension of 200 euros per month, being rated as having a 30% degree of disability. The informant was from the same village as F.M. and knew for a fact that F.M. was not disabled to such a degree. In Kosovo, there are three war associations: 1) Association of the veterans; 2) Association of the invalids; and 3) Association of National Martyrs. The Agency opened a case, and initially sought material from the three associations. F.M. was registered as a veteran-participant of the war, but not as a disabled person. The Agency therefore used its legal right and requested data and accompanying documentation from the Ministry of Labour and Social Welfare concerning F.M. After receiving

the documentation, it was noted that there were essential differences. The basic document for the provision of pension was not original - it was falsified. An IT official was responsible for falsifying F.M.'s electronic file by supplying falsified 'scanned' documentation for obtaining the disability pension. The Anti-Corruption Agency's conclusion was that there was a well-founded suspicion that the officials of this office had falsified electronic data in order to enable a material benefit-disability pension. The case was handed over from the agency to the State Prosecution, which within three months engaged the police in the process of collecting evidence. During the criminal investigation, many more violations were found. More than 1500 persons, by falsifying documentation, had obtained the disability pension as disabled war victims, without in fact being disabled. The wealth of the person leading this office had, coincidentally, increased significantly too. Currently the case is in the process of awaiting criminal charges for the acts sanctioned by the Criminal Code: fraud in office and falsification of official documentation; whereas three officials of the Department of Disability Pension of this Ministry have been suspended without pay. The abuse was committed during the scanning, where the medical report was falsified. F.M. had supplied a document with which he presented that during the war in Kosovo he had medical problems. The document is not from the war period, but was drafted 5 years later. It contained the dates as if it had been drafted during the war. This case shows that it is not enough to have checks in an IT system if the checks do not extend to the paper documents that are fed into the system. Furthermore, possible weaknesses in the IT system might make it difficult to show that a document was scanned and filed with the system afterwards, covering up the whole backdating scheme.

Kosovo case 3: Misuse of the Password

The job vacancy listing for appointing the clinic directors in the University Clinical Centre of Kosovo has failed several times. There is special interest among the medical staff to be in charge of the departments. In some cases, the Ministry of Health and in other cases the Independent Oversight Committee, as the body that oversees civil servants and their hiring or layoff, has cancelled such job vacancies. For years, the majority of clinics have been managed by acting directors, whereas in June 2014, the job vacancy competition was closed. The evaluation committee was established, the questions for the interview were prepared and all necessary preparations for a hiring process were made. In some of the clinics, the directors were appointed, but in eight clinics, no new directors were appointed. One of the candidates for leading a clinic received information that some of the other candidates had received the questions in advance, however, the questions were supposed to be secret

until the day of testing. A member of the oversight committee informed the press[31], and the media published the e-mail address from which the questions had been sent. Being in a tight spot by all these facts and the following scandal, a member of the commission for the selection of directors organised a press conference, and admitted that the data was sent from his computer to some of the candidates, but that he was not responsible for doing so. The official tried to place the responsibility upon a person whom he accused to have stolen and misused his password, and who had accessed his computer in an unauthorised manner, and states that he had given that person his personal password when he went on vacation. However, the outcome of this scandal was that the member of the commission resigned, the job vacancy would be reposted, whereas in relation to the other measures to be undertaken, the Anti-Corruption Agency had yet no information in this regard.

Last year, the Anti-Corruption Agency was unofficially informed that the assistant director of a department in one of the independent mechanisms used the e-mail address of the director in an unauthorised manner. There are several cases when senior officials authorise their assistants to access their e-mail addresses to communicate on their behalf, however, the case in question constitutes an unethical behaviour of the assistant who used the e-mail of the head of the institution from her home, since she was on her maternity leave.

Kosovo case 4: Falsification of tax documents

A cleaning company bids and is awarded the contract for cleaning a ministry building. The whole procedure begins to be implemented according to the legislation in force. The winner with the lowest price is announced; the contract is concluded, and implementation begins. After several months of implementation, the interpersonal relation between the staff of the contracted company deteriorates. The owner of the company fires a person who had worked at the ministry for many years and who was in charge of finance and procurement. Unemployed and disappointed with the situation, this person decides to "retaliate" against the former employer. He decides to denounce the company. One day, the Anti-Corruption Agency received information from an anonymous person through e-mail: the cleaning company owned by a person with a suspicious past wins many tenders for facilities maintenance of Kosovo's central institutions. The informant tells the Agency how this company wins all of its tenders; the essence is that this company does not

31 Daily Newspaper Tribuna, Wednesday August 13, 2014, no. 1538, year 2014, page 10-11 http://www.gazetatribuna.com/?FaqeID=1

pay its taxes and can therefore bid at the lowest price. The proof that taxes are paid on a regular basis is one of the basic documents a bidder has to provide in the tender dossier when bidding for a contract. The owner of the company had used his power to get around this, based on having good relations with tax officials. After one initial payment of a high-value tax, in all future bidding he had used the same receipt but with falsified dates. All officials of the institutions may request the original document, but they were reluctant to ask for it, as they felt they were dealing with a senior person, and provide the excuse that the document is scanned and meets their requirements.

The Agency requested access to information about this company from the Tax Administration. Suspicions proved to be true. Taxes were not paid on a regular basis, and documents that this company used to win the tender were falsified and as such should not have been accepted. The Agency has dealt with many other tenders won by the company, and identified three local and one international institution where this company had been working. Curiously, the company also submitted a bid for the maintenance of the Agency building; however, at the final moment of the assessment of the bids, it was withdrawn without providing any explanation. A criminal report against this company was handed over a few months ago to the state prosecutor. All institutions have been notified about the findings and have received a request from the Agency to terminate their contracts with the company. But despite that, this has not happened everywhere. The international institution has terminated the contract and initiated a case with the EULEX prosecution for compensation of damage. The agency has also requested from the Procurement Review Body - Tenders Court to put this company on the blacklist, in order for the company not to be awarded any other jobs with government institutions. Unfortunately, the Agency has still not received confirmation that similar action has been taken by local institutions.

Macedonia

By Marjan Stoilkovski and Rozalinda Stojova

Macedonia's definition of corruption

In legal terms in the Republic of Macedonia, "corruption denotes using of function, public authorisation, official duty and position for the purpose to gain any benefit for oneself or for another person"[32].

32 Law on Prevention of Corruption, amendments from 2 July 2004 Definition of corruption, article 1-a: http://www.dksk.org.mk/en/images/stories/PDF/law/2004.pdf

Corruption can take place at all levels of government, and its victims can be individuals, or even entire communities. Corruption is a complex crime that often involves more than two parties, therefore making it difficult to distinguish it from other forms of crime; because of this, often, the investigation never treats corruption (including corruption involving the manipulation or abuse of IT systems) as a stand-alone act, rather, it is always related to other criminal offences.

Ranking

Results from the two most recent Transparency International Corruption Perceptions Indices (CPI), show that Macedonia ranked in 69th and 67th place in 2012 and 2013 respectively, which in the regional context puts Macedonia in the second place among ReSPA countries[33].

However, from a cultural and social point of view, it is significant that "the Macedonian citizens rank corruption as the most important problem that their country faces after unemployment and poverty/low standards of living". (UNODC enquiry, 2011)[34]

Year	Country Rank	Country/ Territory	CPI Score
2012	69	Macedonia	43
2013	67	Macedonia	44

Macedonia case 1: Abuse of the IT System on pay tolls

This case is an adjudicated case of abuse of official position and that, according to Macedonian Law, is considered a basic act of corruption. It involves the tampering with a pay tolls IT system, which is used for managing the process of paying the tolls; managing the employees' shifts; and their working processes on pay tolls.

The unit for the fight against corruption and the financial crime unit were assigned to investigate this case. At the beginning of the investigation, the units requested to officially receive all necessary information about the IT system from the company that developed and maintained the management

33 In 2013, this is shared second place with Montenegro.
34 https://www.unodc.org/documents/data-and-analysis/statistics/corruption/Corruption_report_fYR_Macedonia_FINAL_web.pdf

of the pay tolls. The investigation revealed that there was a combination of different types of abuse of the IT system, committed by the employees:

- abuse of the IT system by using different authentication credentials and using the credentials of other employees,
- combined with giving command for vehicle clearance, or
- tampering with the IT system by altering the amount paid, or
- not recoding every vehicle that passed through the pay toll, or
- not giving receipts and sharing the fee with the vehicle drivers by the principle of sharing 50:50, or
- entering a different category for the vehicles.

Special investigation measures were used in order to collect relevant evidence. Data and information collected from the IT system during the investigation helped to identify and prove the illegal activities of an organised criminal group. At the end, and mainly through different analyses undertaken on the data from the IT system, it was possible to assess and calculate the damages by the company.

The investigation showed that there was abuse by people in official positions using the IT system, thus enabling employees to gain illegal profit that in a later phase was being laundered through legal investments in goods.

The criminal charge for this case was submitted on 1 December 2011, and 92 people were convicted for the abuse of official positions and services, forgery, corruption (accepting bribes) and being members of an organised criminal group. By performing such illegal activities, the organised criminal group illegally gained more than 120 million Macedonian denars and caused the company to pay fines for the same amount.

The court procedure was closed on 23 May 2013 with convictions ranging between 3 and 6 years imprisonment for 86 persons, and with sentences including repayment of the damages caused to the company of around 107 million denars. Eleven persons were sentenced to confiscation of their property to the value of 5 million denars.

After this case was finished, the company that owns the pay tolls in the Republic of Macedonia improved the IT system for managing the process of paying toll fees and monitoring the employees' work. The improvements to the system were designed and developed to overcome the identified and anticipated problems by automatisation of work processes, avoiding employee data entry into the IT system, and interaction with the process itself.

Macedonia case 2: Attack on the IT system for public procurement

In the Republic of Macedonia, starting from 1 January 2012, according to article 8 of the Law on Public Procurement, the contracting authorities are obliged to use electronic auction in 100% of published tender announcements for open procedure, restricted procedure, negotiated procedure with prior publication, and simplified competitive procedure.

The electronic system for public procurement is a web-based application where advertisements, notices, and tenders are published completely electronically, and where bidders electronically send their originally submitted offers.

The system is owned by the Bureau of Public Procurement, and is hosted by a local service provider. The system has a firewall installed and is configured with an Intrusion Detection System (IDS), and uses a Virtual Private Network (VPN) to provide secure access to the system. The system itself uses the secure https protocol, and SSL certificates.

At the application level, the system registers different types of users, contracting authorities, and economic operators (companies). The system has its own level of application modules and assigns users appropriate access privileges.

Contracting authorities have their own internal users at application level, i.e. local administrator, procurement unit, public procurement committee, and responsible person. Economic operators (companies) also have their own internal users, all of whom have the same privileges: the ability to share electronic procedures, the participation in electronic auctions, asking questions, etc. One authenticated session by a user on application level lasts for 40 minutes; if there is no user activity during that period, the user is logged off.

In August 2012, an offer for procurement of cars was published using the IT system for Public Procurement. The bidding process was managed by the IT System for Public Procurement, and more than one bidder was submitting an offer. During the bidding process, the IT system was functioning well up until the last few minutes, when the system went down — it was not able to receive any other bids in this period, despite the fact that new bids were attempted to be submitted by users.

The case was first reported as an intrusion into the computer system and a computer crime case. This is procedural practice, which implies that, initially, cases of this kind are investigated as computer crime, while in the next phase of the investigation and if there is evidence for other crimes committed, the case will be investigated for other criminal acts in parallel. Since this incident was a case involving public procurement of high-value equipment, it was considered and treated as a computer criminal case and at the same time as some type of corruption. Even though there was no evidence and information, in the beginning, that corruption or abuse had taken place, the investigation covered both aspects of the case.

The computer crime unit investigated this case and asserts that it took all necessary steps in order to preserve evidence and obtain all relevant information that would help the investigation. In the beginning, basic information from the IT system, detailed technical information, all relevant system, security, and administration logs were requested from the hosting company and from the Bureau for Public Procurement.

The cybercrime unit received the inetpub logs from the server containing records of IP addresses that had accessed the application, application logs and logs during the auction process. After detailed analysis of the provided information using the Linux operative system and bash scripts, it was revealed that in the critical period the system was down due to Distributed Denial of Service (DDoS) attacks performed from numerous IP addresses originating in foreign countries. The investigation also identified that the last bid was submitted by company A just seconds before the system went down, but when company B tried to submit its bid, the system was not available and thus, was not able to accept new offers.

Company B reported the case as potential abuse and submitted the data that proved that they submitted a new bid in the period when the System for Public Procurements was unavailable and that this bid was not registered and therefore had not been accepted.

Later, the investigation revealed that the IT System for Public Procurement was not the targeted web site for the DDoS attack, but the target was another web page (informative web page). Because both systems were hosted on the same server, both web services were unavailable.

Based on the provided logs it was determined that during the critical period, there were many requests being sent to the system that were the subject of the attack and not to the web service running the public procurement system.

A DDoS attack is one of the methods used for making some services unavailable on the Internet. By sending a large number of requests to a system, the system becomes unavailable as it cannot handle and process all the requests. When a system reaches the point of not being able to handle all requests sent, it usually turns itself off. In most cases, this type of attack is performed by using botnets (a network of many computers controlled by one computer with the intent of performing some activities).

This type of attacks does not cause significant damage to the system under attack such as deleting or altering data. It only makes the service unavailable, usually by turning off some system services or by shutting down the system.

At the end, this case was not proven to be an abuse of official position and corruption, but it gives an overview of the procedure and potential methods of abuse of the IT systems for corruption, by abuse of official position or social engineering. Bearing in mind the technologies that are used for facilitating and improving daily work and services, we can identify many modi operandi for abuse of IT systems.

The system administrator has full privileges into systems over a protracted period of time, and if his/her activities are not appropriately controlled and monitored, he/she could abuse the system by destroying or altering the digital evidence, and consequently making it impossible to investigate the case and prove the abuse.

Macedonia case 3: Abuse of IT system and illegal disclosure of personal data

The development of technologies and the implementation of new technical solutions as tools for delivering services in the public sector increase the risks of potential abuse of official position by employees of public sector institutions.

The case described here is an abuse of official position and the permission of access to the IT system that holds restricted data or data which may be disclosed only under specific conditions. According to the national legislation for the protection of personal data, the institution that holds or processes personal data is obliged to follow special procedures for disclosure of personal data.

In this case, an employee in a public sector institution with access to data on the financial incomes system abused his position and disclosed such

information. Although the procedures are stating that information may only be disclosed upon personal request of the citizen or by representatives from a law enforcement agency upon a court order, in this case, the employee did not respect the procedures for disclosure of personal data, and issued an official document generated by the IT system containing personal data. Later, this official document was used as evidence in a civil litigation process.

This case was investigated from three aspects: abuse of personal data by the employee and the institution (investigated by the Directorate for the Protection of Personal Data); abuse of official position and service of the employers (possible corruption, i.e. the receiving of a bribe or in order to obtain other benefits and advantage); and abuse of personal data according to the National Penal Code, article 149 on the abuse of personal data (investigated by the Ministry of the Interior).

From the investigation that was conducted for abuse of personal data and abuse of official position, evidence was collected showing that the employee had illegally issued a document from the IT system and that he/she committed a criminal act. The evidence was extracted both from the IT system and from the surveillance camera system (CCTV). Although in this case, the receiving of a bribe or the obtaining of other benefits and advantages was not legally proven, the fact that the employee had the permission to use the system but had no authorisation from the data owner to release it, was considered by investigators (the police and the prosecutor) as a form of corruption, as defined by national legislation.

This case is just one example of abuse of official position and there are many similar cases like this, i.e. the abuse of official position to disclose information. The fact is that often such cases are not being reported as criminal acts, but are only investigated internally within the institution.

Macedonia case 4: Misuse of registering working hours system

In the last decade, systems that register working hours have been incorporated in the daily work of many institutions, public enterprises, hospitals, and schools. Systems register the arrival and departure time at the workplace, as well as official and private absences, and stored data is being used to count the number of working hours for employees over a certain period of time. The number of working hours is used to calculate employees' salaries, determine periods of continued absence by an employee, and for other analyses. According to relevant laws, staying at work after the defined working hours, does not mean

overtime by default. On the other hand, repeatedly being late for work in a short period of time is a reason for initiating disciplinary proceedings. This is particularly applicable in institutions that work in one shift, knowing that in Macedonia there are no "sliding" working hours in the administration.

In one of the institutions where such a system was installed to register the working hours, only one person was assigned the role of administrator responsible for managing the entire system. Administrators' privileges include the opportunity to inspect and preview attendance records and to generate general reports and specific reports such as for a specific employee, a group of employees, or reports for a certain period.

After playing the role of an administrator for more than two years, the employee recognised the opportunity to exploit the system to his/her advantage in a way that he/she could change the times of arrival and departure so they correspond with the legally defined ones, rather than the actual ones. The employee was doing this for over a year and a half without being noticed by colleagues or supervisors. One day, the need arose for the employee to change data for that morning or for the last working day, without checking how the data is being managed and kept in the system, especially without checking how the administrator's activities were recorded. Although rare, on occasion, the opportunity for misusing the system was used for more than just late arrivals, but for whole days.

Nearly two years after being assigned the role of administrator, the institution performed a reassignment of tasks among employees, resulting in a different person becoming the administrator. The new administrator accidentally opened the records of events (logs) and realised that some of the events were marked, making them different to others. Interested in finding out how they differ from the remaining ones, the new administrator began to review the records in detail. It became clear reasonably quickly what the marked events meant and he/she reported it to management.

The process of investigation began with the appointment of an official IT person from the institution, whose main task was to review all reports and event records (logs). The conclusion of this procedure coincided completely with the assumptions made by the newly appointed administrator.

Due to the confession of the employee, the case was not prosecuted and was resolved internally. There was an assessment of the financial damage he/she made by not coming into work and failing to complete tasks, and for that amount the employee was punished with adequate disciplinary measures. But the employee's contract was not terminated.

Macedonia case 5: Abuse of administrator's rights

In the process of issuing licences for imports, among a list of required documents, one must also submit a bank guarantee on the value proportional to the value of goods or services being imported. The rules are very strict, the higher the bank guarantee, the higher the value of imported goods that is allowed.

The system for checking the data at borders and issuing licences uses the data entered, stored, and kept at the administrative centre of Institution A. While some of the data is collected based on the exchange between this system and systems of other institutions, the value limited by the actual bank guarantee is entered by the administrative officers rather than the banks information systems.

One administrator, between his transfers from one administrative centre to another, discovered a way to benefit from his position. After his movement from administrative centre B to administrative centre C, he notices that his access privileges are still the same, so he creates a new user account for himself. The super administrator did not perform regular checks and revisions of the privileges of re-allocated administrators, and the administrator was thus able to commit many offences using his newly generated user account.

Over a period of two years, and by using the fake account on over 100 occasions, and his own account for a dozen more, the employee entered higher values of the bank guarantee before checks at the borders, and returned the real values after the checks. When the border officials checked their system, data altered by the administrator appeared as prescribed by the law. He stayed in constant contact with the management of the company in order to know exactly when the goods would arrive at the border. For the shortest period possible, the records in institution A held declarations of higher bank guarantees.

The case was detected by the internal control and audit together with the ICT department while performing regular audits. An investigation team was formed to look into the case and identify that this was indeed a case of corruption, if other crimes has taken place, and to what extent crimes were committed.

Analysing events in the system logs, the IT investigation team determined the IP address from where the changes were done, which led them to the administrators computer. Log-files could not be changed, so it is very easy to make a list of actions performed by the administrator.

That the act was premeditated was further revealed by his choice of account name and password. He ensured that during regular checks, the account and password would be among the last ones to be checked and were ones that did not stand out, thus avoiding any suspicion being raised.

It has only been proven that he used this way of abusing the system of Institution A in cooperation with one local company. The financial damage to the country was assessed to be to the amount of 10,614,779.00 denars.

Montenegro

By Dusan Drakic and Ivan Lazarevic

Montenegro case 1: Abuse of office and forgery of official documents

The case in question is an example of negligence in the workplace and illegal conduct of a state authority, i.e. abuse of authorities and office by persons employed in that authority.

The passport of a person "A" had expired and he received a new passport. Officials in the competent authority of the Ministry of the Interior of Montenegro decided to use the old expired passport for criminal purposes. Using the stamp of that authority, they extended the validity of the old expired passport for five years under the name of "A", but with a photograph of a third person "B".

Apparently, "B" was wanted by the police. As a consequence, "A" was retained at the passenger terminal at the airport in Lisbon, where he was about to board a ship to work for the coming period. After checking his identification documents, a police intervention team led him (handcuffed) to the Emigration Centre at the airport, where he spent 48 hours, by which time the police (hand-tied) put him on the airplane out of Portugal to Belgrade via Switzerland. He had not seen his documents until his arrival in Switzerland. The treatment by the Portuguese authorities and the image created of him as a criminal meant the person "A" suffered mental anguish, and his reputation suffered in his hometown, in his family, among friends, etc.

Failure by the authorised person to destroy the expired passport, and actions taken to extend the validity of the passport under the same name, but with a photograph of a third person ("B") and certifying it with official stamping,

represent actions that constitute the criminal offence of abuse of office and at the same time confirm illegal conduct of the state authorities.

In this case, the officials in the competent authority of the Ministry of the Interior did not destroy the passport, which upon the issuance of a new passport was taken from "A", a citizen of Montenegro.

The court of first instance in these criminal proceedings concluded that failure by the authorised persons to destroy the expired passport, and the following actions explained in the previous paragraphs, represent actions that constitute the criminal offence of abuse of office, under Article 216, paragraph 1 of the Criminal Code of Montenegro, and the criminal offence of forgery of official documents, under Article 207, paragraph 3 in connection to paragraph 1 of the Criminal Code. At the time, the offence was stipulated with a sentence from three months to five years imprisonment. In accordance with Article 216 of the Criminal Code of Montenegro, the abuse of office takes place if an official, using his/her functions or authorities, exceeding the limits of his/her official authorities or fails to discharge his/her official duties, obtains for himself/herself or another person any benefit, causes any damage or seriously violates the rights of another person.

Following the submission of the appeal on the first instance decision, the Supreme Court of Montenegro upheld the primary court verdict and in the reasoning of the judgment, no. 902/13 dated 12 April 2013, clearly stated that:

"all facts stated also confirm illegal conduct of the authority of the defendant - the competent services of the Ministry of the Interior of Montenegro located in Cetinje, which caused damage to the injured party, for which pursuant to the provisions of Article 172, paragraph 1 of the previously valid law on Contracts and Torts the defendant is responsible and pursuant to the provisions of Article 154 of the same law shall compensate the damage incurred. In presenting its conclusion, the Court also invoked the contents of the previously presented concrete actions in this case that constitute illegal conduct of the victim's authority and all other circumstances of the case, as well as the fact that the identity of the third person, who abused the former official document of the plaintiff and his identification data, has been confirmed, and that that person was suited for several crimes committed on the territory of another country (Italy)."

In the course of the proceedings, the victim proved that, due to the illegal conduct of the defendant's authority, he also suffered non-pecuniary damage due to the harm caused to his reputation, honour, violation of freedom and rights of personality.

Also, invoking the data obtained from the concerned shipping company on the amount of earnings (on all grounds) of the plaintiff, earned during the sailing period (and exempted for the disputed period), and the rules governing damages by criteria on the date of sentence (Article 189 paragraph 2 of the LCT), the amount of the related material damage to the plaintiff was correctly determined by a financial expert engaged by the court.

Conclusion 1

The above example shows that there is a flaw or failure in the information system for the issuance of passports. The system should, but fails, to eliminate the risks of passports being used or issued after the validity period has expired. Also, it is obvious that such a document could not be extended without subsequently entering incorrect data in the information system for the issuance of travel documents. It is interesting that there are no electronic traces of the officers who issued such a document. Data should be available in the information system regarding the date, time and name of the officer who accessed the system and processed and issued the document. The above also indicates that the system for issuing and control of travel documents, particularly at border crossings and airports, must be capable of analysing and eliminating such falsified documents if they appear in the system. Identification numbers of such documents should be automatically identified and permanently removed from electronic records, and the IT system itself should be able to recognise them as invalid (even though this data would only be useful in Montenegro, not in foreign countries).

To solve this and similar issues, it is necessary that all IT databases are regularly updated and linked to the greatest extent possible, so that the identification number of such documents would be electronically eliminated from further use or abuse by human factors. However, there still remains a risk if such a document is physically transferred to a third country, and used as valid there, which raises the question of the need for regional IT cooperation, with the aim of eliminating potential risks.

Montenegro case 2: Using IT data to inflict political damage

In order to provoke political destabilisation and discredit certain senior government officials/politicians or obtain personal gain, an alleged telephone listing of members of organised criminal organisations, which contained phone numbers of the senior government officials/politicians, was published in the media. The intention was to influence public opinion by

indirectly linking the officials with the organised crime group in question, so as to create an image of an alleged connection between the state authorities and organised crime.

At the end of 2011, the listing was sent from two local post offices to a daily newspaper, as well as electronically from an IP address on a wireless network located in the building in which a senior public official lives. The daily newspaper published the alleged listing, according to which the chief of the criminal group, for whom an Interpol arrest warrant was issued on charges of drug trafficking, had telephone communications with several government officials in Montenegro. What is particularly interesting is that the listing refers to telephone communication of the chief of the criminal group from 2008, and has been kept for three years until it was published. It further deepened suspicions and speculations that someone from the operational structure of the police/internal affairs/safety sector was involved in the case, led by greed or revenge-seeking, in order to cause political destabilisation in the country on his own account or on the account of still unknown persons.

The case has not been brought to court, as the investigation found that there was no telephone communication between the senior government officials/politicians and the main organiser of the criminal group, and that the listing was forged and was not a police document, as presented in the media. Furthermore, the telephone company made it clear that the published listing, which the daily newspaper claimed the mobile operator had submitted to the police for investigation, was not a listing from the company, i.e. did not comply neither in form nor in the content with the ones in which data on communication traffic are reported at the request of the authorised body, in accordance with the existing legislation of Montenegro. It was found that the listing of the person designated as the main organiser of the criminal group, and made by the Police Directorate for their investigative/operational needs, was subsequently forged, i.e. containing the names and numbers of senior government officials and their addresses.

However, it is still unknown who was providing the original listing or the one that the police creates for their operational needs, nor who the forger was that made the list look authentic. Neither is it clear how and on which grounds the Police Directorate obtained the listings from 2008, and what kind of investigation was conducted then against the mentioned main organiser of the criminal group, nor what the results of the investigation were and what kind of evidence was collected at the time.

What also remains unknown is the person who sent the materials, i.e. e-mail messages from the aforementioned IP address.

This case represents a classic example of the violation of basic human rights guaranteed by the Constitution and international conventions, violation of rights of privacy, possible abuse of powers, because the listings of conversation cannot be obtained without court approval, nor be published in the media. Also, this case represents, with a great possibility, the case of bribery and abuse of office, as well as falsifying of data and IT system abuse.

Conclusion 2

The above example clearly shows the vulnerability of IT systems and possibilities of its abuse. It primarily concerns the constitutional principle that applies to the inviolability of the confidentiality of letters, telephone conversations, and other means of communication. On the other hand, there is the issue of potential liability of the responsible persons in the operator company, primarily in relation to the confidentiality and the interception and abuse of electronic mail. The operator is obliged to provide required technical and organisational preconditions that allow the interception of communications, i.e. to enable the relevant state authorities to obtain retained data on traffic and location, but solely pursuant to the court's decision, if it is necessary for the conduct of criminal proceedings, or for reasons of security of Montenegro. The public did not get answers to whether such approval existed and which proceeding was led by police at the time and why. The case proved to be extremely complicated, because in addition to the potential elements of abuse of powers it also has elements of cyber crime, which requires a high level of knowledge, training and technical capacities, as well as quality international assistance.

The case did not have a court epilogue nor provided answers to a series of the above questions. No objective or subjective responsibility was established. Certainly, in addition to the political damage that has been caused by these events, what is even more important is the fact that if such a case, regardless of the motives and reasons, could happen to the highest state officials, what could an average citizen of Montenegro expect, if he/she find himself/herself in the same or a similar situation.

We should also mention the inadequate and insufficient reaction from state authorities in relation to determining objective responsibility for the work of institutions and the ability to discover offenders, which undoubtedly causes immeasurable damage to the country and the general principle of the rule of law, manifested in the loss of trust of citizens in the work of the institutions. It is required to put additional efforts and thoroughly analyse the existing system in order to establish clear procedures for obtaining and using operational data and to establish clear and specific preventive measures,

with the use of software and IT capabilities. In particular, it is necessary to continue to improve communication with the public and the media in such cases in order to raise public trust in their work.

Montenegro case 3: Abuse of functions and entering incorrect data in public registries

This case is related to the electronic production of false licenses or other certificates, in order to use such a certificate in legal proceedings.

By a judgment of the Basic Court in Kotor from 2010, two persons, an officer and the head of municipal cadastre of a municipality in Montenegro, were found guilty of criminal offence of abuse of office, as per article 416, paragraph 3 in connection with paragraph 1 of the Criminal Code of Montenegro. The judgments stated that they have been using their positions to obtain illegal gain, and exceeded the limits of their official powers by making and publishing decisions for which they had no authority. By first decision they enabled the restitution and the transfer of state-owned land to the land's alleged previous owner, who registered the land in the electronic land registry, and sold the land immediately after registration. At the same time and in the same way they issued another decision with false content, by which time some other specified land was returned to its alleged previous owner. In this case, the alleged owner sold it immediately after the unfounded registration, even though the owner did not have a valid title deed, with the help and signatures from the accused persons. By performing and enabling such actions and with the land restitution, the accused persons obtained gain in the amount of 571,307.32 euros.

Those two persons were sentenced to two years' imprisonment.

It has been proven that both defendants in the particular case had exceeded the limits of their official authorities. Also, it has been proven that the procedure of the restitution and the transfer of the land was not preceded by a decision of the local Parliament, as well as that the decision was rendered without the requirement of authorised persons, the former owners, avoiding the procedure foreseen for the administrative procedure. The following acts resulted in the adoption of decisions in the cadastre, where quite obviously the procedure was not complied with, nor represented the interests of the municipality protected.

The Criminal Code of Montenegro defines the criminal offence of abuse of office as exceeding the limits of his/her official authority to obtain unlawful material gain over 30,000 euros.

Therefore, the court ruled that the defendants (an officer and the head of the municipal Cadastre) acted without authorisation in those cases. They knew they were not authorised for restitution and could not transfer the land to its alleged previous owners. They also knew that the land was under the jurisdiction of another municipal authority. Additionally, the evidence showed that the decisions brought by the defendants were not supported with documentation proving ownership of the alleged previous owners to which the land was returned. Further, the following procedure of restitution was performed upon oral request of a person who had bought the land from the alleged previous owners despite the fact that the following land is nationalised property and could not be up for sale. For the court it was undisputable that both defendants exceeded their authorities, the procedure stipulated for administrative proceedings was not pursued, nor were the interests of the municipality protected, and thus both defendants committed the criminal offence with which they were charged.

Conclusion 3

The above example clearly indicates that data from public registries, kept electronically, may be subject to manipulation by those authorised to use them and enter data therein.

Entering data into electronic land registries was preceded by the adoption of an unlawful decision, so this case could constitute not only the criminal offence of abuse of office referred to in article 416 paragraph 3 in connection with paragraph 1 of the Criminal Code of Montenegro, but perhaps also some of the offences relating to the security of computer data. Because of this, it is clear that potential land buyers can be misled when checking data in land registries, and then be exposed to subsequent litigation for determining the rights of ownership, where the slightest flaw in the conscientiousness of the acquirer or buyer of the property may cause significant material damage.

In this case it was clearly demonstrated that, following the decision of the municipal Cadastre, which does not have the authority to make such decisions, changes have been made to the database cadastral records. The case proves that the existing IT system and the procedure of keeping records, in particular access modes to databases and the IT system, and the possibility to make changes in records without a valid legal basis, is incomplete and inadequate. It is essential to improve the IT system in a way that would clearly and unambiguously determine the access procedure, as well as the authorities under whose decisions the access and the changes of the data in the records are possible.

Montenegro case 4: Illegal issuance of travel documents

An employee in the Police Directorate of Montenegro, in Podgorica, in the capacity of a clerk in the Department for Travel Documents and Weapons, was accused of using her official position in order to gain benefit for other persons during 2004 and 2005. The clerk acted contrary to the Law on Travel Documents and Decision on the issuance of passports, common passports, travel certificates and visas, after receiving a request for the issuance of two travel documents (passports), and completed the documents without previously checking the identity of the applicant or person for whom the issuance of travel documents was requested. She did not conduct verification in accordance with the above regulations either. She therefore committed the criminal offence of Abuse of Office from article 416 paragraph 1 of the Criminal Code.

It is interesting that in the first instance decision, the court, taking into considerations the charges, the defence and all the evidence, found that the defendant should be exempt from prosecution pursuant to article 363 paragraph 1, point 1 of the Criminal Procedure Code - as the offence for which she was accused did not constitute a criminal offence under the law. In the indictment the emphasis is placed on the fact that the defendant took actions in order to obtain gain for those persons, but the factual description of the offence omitted the part that refers to the fact that the passports in questions were issued to persons indicated in the indictment, and in this regard it omitted the part that relates to the gain obtained to these persons.

A particularly interesting detail from the judgment is that the defendant stated that although she had access to the travel documents in question, there were no records of the travel documents, nor were any applications found. They had all disappeared. When her supervisor ordered for the documents to be sought, they found that all documentation had disappeared. An internal investigation could not identify anyone involved with the disappearance, nor what had happened with the documentation. The fact is that the documents were kept in the filing room, located in a basement room of the Security Centre, and guarded by a special officer. However, all employees in the Department have access to the filing room. The defendant therefore speculated on what grounds her former superior officer concluded, that out of seven colleagues, she should be the offender.

During the procedure, the Criminal Code was amended. The offence with which she was charged no longer constituted a criminal offence in accordance

with the amendments. In accordance with article 133 paragraph 3 of the Criminal Code, the court was therefore obliged to apply the law that is most favourable to the defendant. Accordingly the defendant was found not guilty for the offence in question and the process was returned for retrial.

A new proceeding was initiated. It involved not only the aforementioned officer, but also two other officers from the Police Directory / Ministry of the Interior. The two new defendants were charged with using their official authority to forge and issue a large number of ID cards, driving licenses, and passports between 2011 and January 2013. They were also charged with subscribing persons for whom they had issued legitimation for in the Registry of Montenegrin Citizens. Finally, they were charged with receiving bribes for each issue of false documentation to the amount of 50 – 1,300 euros. In total, the indictment charged 17 persons for corruption, i.e. giving bribes and forging documents.

Two persons were charged with mediating in receiving bribes. They would look for citizens who needed such documents, and for a fee to connect them with the accused officers.

Another person, a computer science engineer, was charged with forgery of documents. He would, in agreement with the above helpers, create false certificates of passed driving exams.

Seventeen persons were charged with paying bribery and forging documents.

The entire case was completed in Court in July 2014. The clerk, as the main accused, was convicted of receiving bribes, exercising unlawful influence, and having helped forge documents. She was sentenced to a single sentence of four and a half years in prison.

Overall, the final judgment of the Special Council of the High Court in Podgorica, sentenced the 17-membered group to a total of seventeen years and four months in prison for forging documents, and giving and receiving bribes.

Conclusion 4

The above examples also show that there is, or there was, a flaw or omission in the Ministry of the Interior document management system. There are no electronic records of scanned requests for issuance of passports in the information system, which would eliminate the risks of using and issuing

forged documents. It is also obvious that there are no electronic traces that would show who issued such documents.

As a possible solution to this and similar cases, it is necessary to introduce document scanning or establish electronic databases of all documents submitted and issued in hard copy with mandatory double back up option, to ensure the security of data in the event of their intentional or accidental destruction. Also, it is necessary to improve the electronic system security recording physical access to premises where files and official documents are kept.

Summary

In summary, note that when it comes to the criminal justice system in Montenegro, corruption crimes are stipulated as criminal offences against official duty in Chapter XXXIV and XXII of the Criminal Code. As such, these criminal offences are nothing more than different forms of abuse and a deviation from the law-defined manners of performing duties. Therefore, criminal corruption offences pose a greater threat to society as the perpetrators are primarily public officials. Through their actions they violate the legal and administrative system and reduce the efficiency of the state. In addition to the obvious material consequences incurred by such offences, the most harmful consequences include threats to the integrity of the institutions and a decline of public trust in the work of state and local authorities. That is, ultimately, the functioning of the state.

The Criminal Code of Montenegro prescribes the following corruption crimes:

- money laundering (Article 268 CC); violation of equality in the exercise of an economic activity (Article 269 CC);
- abuse of monopoly position (Article 270 CC);
- abuse of office in business operation (Article 272);
- causing bankruptcy (Article 273 CC) and causing false bankruptcy (Article 274 CC);
- abuse of authority in economy (Article 276 CC);
- passive bribery in business operations (Article 276a CC);
- active bribery in business operations (Article 276b CC), false balance (Article 278 CC);
- abuse of assessment (Article 279 CC);
- disclosure of trade secrets (Article 280 CC);
- disclosure and use of stock exchange secret (Article 281 CC);
- abuse of office (Article 416 CC);

- negligent performance of duty (Article 417 CC);
- fraud in service (Article 419 CC);
- unlawful influence (Article 422 CC);
- incitement to unlawful influence (Article 422A CC);
- passive bribery (Article 423 CC);
- active bribery (Article 424 CC).

Generally, such crimes are punishable by imprisonment, and confiscation of proceedings obtained where possible. However, in practice, these criminal offences are often linked with other criminal offences, that in essence are not corruption crimes, but are closely linked to them. This includes forging of official documents and offences relating to the security of computer data. It seems that in the case law, there are still not enough examples of corruption offences abusing computer data, but practice will show how adequate existing legal safeguards are, and whether there is a need to introduce new offences related to computer crime.

Certainly, the fact remains that one of the mechanisms to combat corruption effectively is successful criminal prosecution. This implies effective methods for detecting and collecting evidence, and having effective and adequate sanctions.

The competent institutions for detection, prosecution, and sanctioning in Montenegro are the police, public prosecutor and courts. These institutions are functionally connected and each of them, within its scope of competences, applies prescribed legal institutes in combating corruption. However, they sometimes encounter difficulties in applying such institutes, which call for various professional discussions and amendment of laws in the field of corruption. Police, as the authority responsible for the detection of crimes, needs the cooperation and involvement of other institutions: primarily banking and other financial institutions, the Directorate for Anti-Corruption Initiative, the Directorate for Prevention of Money Laundering, the non-governmental sector, and citizens themselves. On the one hand, the police are authorised to apply the broadest methods of gathering evidence, i.e. the measures of secret surveillance for criminal offences of corruption, regardless of the manner of execution of criminal offences and the prescribed punishment. On the other hand, such methods also raise the question of potential violations of basic human rights and privacy.

Regardless of these suppressive measures, prevention of corruption is of great importance. It basically entails raising the level of awareness, knowledge, and skills, as well as the responsibility of employees, on one hand, and provision of adequate physical, technical, and financial conditions of employees on the

other hand. Thus, one of the modern preventive methods for providing and establishing legal and ethical quality of work in state bodies is the preparation of integrity plans for institutions. They represent internal preventive anti-corruption documents, mapping vulnerable areas in institutions, i.e. risk analysis of work processes in each state body, organisation, or service. Finally, integrity plans should be understood as a form of strategic, quality and risk management, which should result in higher quality of services in public sector, decrease of costs and increase of the resilience of institutions to illegal and unwanted effects. This includes digitisation and IT use as one of the key elements.

Serbia

By Nemanja Nenadic and Bojan Cvetkovic

Conducting the study on IT-related corruption, the following institutions were contacted for interviews:

- Ministry of Justice
- The Office of the Commissioner for Information of Public Importance and Personal Data Protection
- The Directorate for e-Government
- The Ministry of the Interior
- The Ministry of Finance
- The Ombudsman

Only the first two institutions answered the call and meetings for interviews were arranged. The Directorate for e-Government answered the call, but an interview has never been arranged.

Serbia case 1: Sex at Belgrade Arena

At the beginning of March 2011, video footage showing sexual intercourse in front of the Belgrade Arena was published on the Internet. The footage itself was recorded early in the morning on 24 April 2010. As the footage had been recorded by a video surveillance system used by the Ministry of the Interior (MoI) to control traffic in Belgrade, this represents a clear case of an "abuse of office" corruption offence.

The first reaction of the people involved in the original footage published on the Internet was relatively mild, but in the months following the incident, it became quite clear that the footage had impacted considerably on their lives, and the lives of their families. The identity of Elizabeta M. (22) and

Milovan S. (24) were publicly revealed, and they had to literally avoid any kind of public appearance, and their families, according to their own claims, "went through hell".

The Commissioner for Information of Public Importance and Personal Data Protection Rodoljub Sabic (Commissioner) submitted a complaint to the Higher Prosecutor's Office in Belgrade against an "ordinary police officer" for publishing footage of sexual intercourse between two adult persons on the Internet, using recordings from a video surveillance system used by the Ministry of the Interior (MoI) to control traffic in Belgrade. He stated that it was clear that the MoI did not take all the technical, human and organisational precautions to protect data preventing potential misuse of the video surveillance system recordings. In this particular case, IT had been abused by illegally obtaining the data through manipulation of existing data and procedures. At the time when this happened, the only regulation broadly covering this case was an internal MoI Traffic Police regulation saying that video surveillance footage can only be used internally within MoI for investigating the circumstances of traffic accidents. It is important to notice that there were no national regulations covering this case. Also, the key internal high-level MoI policy *"if something is not clearly regulated either by national or MoI internal regulation MoI employees have to ask MoI for official permission instead of assuming they can do that something"* was manipulated.

"It is about an event that is a very grave violation of privacy and a serious violation of the Act on the Protection of personal data", the Commissioner said, adding that the absence of necessary procedures and the existence of security flaws led to the incident.

In line with his duties, the Commissioner initiated an inspection of how the Law on Protection of Personal Data is enforced and implemented by the MoI, which ended with the MoI being issued a warning, which also contained a list of 14 measures and actions to be taken at the technical, personnel and organisational levels to protect data in order to avoid any kind of abuse in the future. The Commissioner also requested that the MoI officially inform him within 15 days of the legal deadline about planned measures and activities that MoI is going to adopt and carry out to eliminate irregularities. On this occasion, the Commissioner recalled that Serbia has no law on video surveillance, although there are a very large number of people involved in video surveillance.

The initial reaction from the MoI was that it would be very difficult to determine who copied the footage and published it on the internet, because heads,

operators and administrators in the Command Operations Centre (COC) all had access to the video surveillance system recordings which, together with the absence of data access and security procedures, presented a clear weakness in the administration of the MoI COC video surveillance system.

After the warning issued by the Commissioner, the MoI took concrete steps punishing the persons involved in the incident. An internal investigation determined that there were 10 computer workstations from which the footage could have been copied (downloaded).

Disciplinary procedures for abuse of power were conducted against the police officer involved, who had been on supervisory duty at the Belgrade MoI COC on the day the footage was recorded. The MoI published detailed instructions in the official guide "Mandatory conditions for use and maintenance of video surveillance of city roads and intersections in the city of Belgrade," in order to close existing gaps in the security system (such as the fact that too many people had access, the lack of records on who accessed what part of the system, etc.), not only for the Belgrade MoI COC video surveillance system, but also for similar MoI systems throughout the country. However, the MoI did not publish details of the investigation and disciplinary proceedings so we do not have insight into the possible motives of the perpetrators.

The Commissioner reacted promptly to the MoI actions, commending them on a constructive and useful reaction to his warning saying that, although by today's data protection and safety criteria the steps taken are nothing special and are considered standard, they, in the specific Serbian conditions, are welcome because they undoubtedly represent a good and useful thing.

Although there had not been similar incidents in Serbia in the immediate aftermath, 2014 elevated the problem of video surveillance system recordings to new heights.

Between 8 June and 10 June 2014, two pieces of footage appeared on YouTube. In the first, a traffic accident that occurred on the night from Saturday, 7 June to Sunday, 8 June 2014 in the city of Novi Sad was shown. The footage showed the moment when an Audi driven by DV (aged 21) crashes sideways into Polo, killing two girls, ML and VM, and a young man, AM (all aged 20).

The second clip attracting public attention came from the city of Niš and showed a pedestrian, MZ (aged 17), being hit by an Audi on the pedestrian crossing, and, as a result of this hit, suffering heavy injuries.

Both footages were broadcast by several domestic media outlets, together with the publication of personal information of all persons involved.

The related Commissioner in charge immediately conducted an inspection and supervision of the MoI Traffic Police Department in Novi Sad, the Novi Sad Public Communal Enterprise "Informatika", whose public video surveillance system had recorded the footage of the Novi Sad car accident, and the MoI Traffic Police Department in Niš. The Commissioner pointed out that "we are faced with a real danger that many CCTV systems turn into a production of horror and scandal", urging the media "to question the ethical standards of their own profession". According to the Commissioner, objective information to the public can be provided without undue intrusion into the privacy of the persons involved, and without adding to the loss of their loved ones. He reminded the police and other state authorities again of the provisions of article 42, paragraph 3 of the Constitution, which explicitly prohibits and punishes use of personal data beyond the purposes for which it was collected — in this case, to contribute to road safety and to assist in detecting and proving the crime.

The families of the victims from Novi Sad and the family of the seriously injured juvenile from the city of Niš stated that the publication of accident footages in which their children were taped was very important to the public, pointing out that people need to see how these accidents occur, but also to reduce the possibility of any kind of cover-ups.

Although at the moment of writing, the results of this inspection and supervision are not yet known, lessons learnt from this case include that Serbia should create and adopt a law on video surveillance that must be in line with the new version of the Law on Personal Data Protection[35] and EU directives in this area.

Serbia case 2: When IT contractor "takes root"

The current Ministry of Justice (the new MoJ) of the Republic of Serbia inherited the duties of the former Ministry of Justice and Public Administration (MoJPA) in a merger of the previous Ministry of Justice (previous MoJ) and the public administration part of the previous Ministry of Public Administration, Local Self Government and Human Rights (MPALSGHR).

The previous MoJ mandate (as in *"terms of office"*) lasted until July 2012. MoJPA was formed on July 2012, and existed until April 2014, when the new MoJ was formed.

35 https://docs.google.com/viewer?url=http%3A%2F%2Fwww.poverenik.rs%2Fimages%2Fstories%2Fmodel-zakona%2Fmodelzzpl.docx

For almost 10 years of public governance in Serbia, the justice function of the government was located at the previous MoJ, followed by less than two years of joint governance between the justice and public administration functions. However, as a result of the last governmental reorganisation, the justice function is now back within the single function of the ministerial body of the new MoJ.

The justice sector with all its inter-related, but independent entities, is a highly complex environment, where each entity within the sector has its own clearly delineated functions, processes and responsibilities, and where interactions with other sector entities are highly regulated. The MoJPA, as well as the new MoJ, had the firm belief that in order to successfully manage and govern the justice sector, ICT should be used just as a tool to reduce the sector complexity. The strategy of the previous MoJ was quite the opposite and directed towards creating complex ICT systems that map the complexity of the sector, requiring considerable budget investments both for operative and maintenance costs. Such actions led to the wide diversity of the hardware, software and related ICT systems used within the justice sector ICT ecosystem, which is still causing big problems concerning ICT contractor-related risks and related opportunities for corruption.

Currently, and according to the Assistant Minister in charge of IT of the new MoJ, there are three different main information systems in the justice sector, using two different application software platforms; two different database platforms; and one operating system platform, although they all belong to a single family of IT application - document management. If one counts the numerous smaller systems, as for example the one used in the Constitutional Court, the number is even higher. These have spurred spending of more than 10 million euros of donors' money, and have also impacted on the Serbian budget for operative and maintenance costs with 1.5 million euros per year! This could have been acceptable if the entire justice sector had been covered by any or all of these three different main information systems; however, the current sector coverage is less than 25 per cent. The bottom line is that in order to cover the rest of the justice sector entities (i.e. 75 per cent), new investment between 20 and 30 million euros is necessary. Such funding is not available to the new MoJ, as it would make the yearly budget for operations and maintenance skyrocket to more than 3 million euros. It is quite clear from the facts above, as well as the fact that the global financial crisis has also influenced the resources available through budget cuts, that finding such resources is difficult. The new MoJ has considerable problems regarding ICT contractor-related risks, something that easily leads to the occurrence of corruption offences.
There were problems during the public procurement of network and communication services (Internet and VPN WAN), which fall under IT

corruption, and could specifically be described as “abuse of office”, “nepotism and favouritism”, and “procurement violations” by the employee of the previous MoJ, and in favour of the very same IT contractor the previous MoJ used as the provider of a single countrywide network and for communication services. An employee of the previous MoJ in charge of computer network services manipulated the procedures defined in the contract between the previous MoJ and IT contractor in a sense that control and safeguard procedures were either not followed or were greatly simplified in favour of the IT contractor and in order to cut his expenses. He also abused the office by both hiding (making unavailable) data regarding IT contractor access to the VPN WAN system and destroying electronic documentation of the system so that the MoJPA and new MoJ could not control, monitor and supervise the system.

The same employee of the previous MoJ showed nepotism and favouritism making procurement violations when he used the data and information about the system not available to the higher officials of the new MoJ to create tender documentation for the new tender for procuring network and communication services. However, the Minister of the MoJPA did not allow this tender documentation to be published because he was afraid of negative effects of the tender that could be potentially rigged in favour of one Internet Service Provider (ISP), the IT contractor, which, at the time of the tender, had already been providing countrywide network and communication services (Internet and VPN WAN) for eight years. Instead, the MoJPA minister gave an order that a new and fair tender documentation be prepared obeying the related laws and using best practices.

Financial damage was inflicted on the new MoJ and on Serbian taxpayers, as the IT contractor did not initially want to re-negotiate the price and the quality of the service, nor allow the new MoJ to initiate a new tender procedure. The IT contractor had managed to stop the new tendering by utilising a complex and exhausting complaining scheme made available by the loopholes in the Law on Public Procurement in force at the time. The employee of the previous MoJ, when faced with the reality, left the ministry during the MoJPA terms of office. MoJPA had initiated a formal investigation and brought the case to the court (the representatives of the new MoJ are handling this case at the moment).

The conclusions that should be drawn from this case are that public organisations must not underestimate IT contractor-related risks. They must have properly prescribed procedures when outsourcing. As the private sector will deliver more IT services in the future, given that governmental organisationžs internal manpower budgets are being cut, IT contractors will become even more important.

Serbia case 3: A senior public official spying on employees

In order to find out who was talking about her poor performance, the General Manager of the Privatisation Agency (Agency) at that time, replaced the IT manager of the Agency for refusing to copy emails from employees, and subsequently, ordered another staff to do so, thus gaining access to a considerable amount of staff emails. This case of "abuse of office" led to her premature retirement and thus, the end of her tenure as General Manager of the Agency.

The now retired General Manager of the Agency, requested copies of business emails from all Agency employees without their knowledge, thereby violating their privacy. Serbia currently has no regulation regulating the ownership of and access to the electronic communication made by employees during working hours, which is why any kind of such communication (e-mail, chat, telephone, social media etc.) is considered to be employee's personal ownership. This is why many companies that are working in Serbia implement their own internal policies and procedures in regard to employee's rights, duties, and obligations regarding electronic communication. So, although these were business emails and she was the Agency General Manager, it was not allowed for her to read them because the Agency did not have related policies and procedures. It is not known who now has access to the hundreds of thousands of emails from 300 employees downloaded after business hours and on weekends. It is also not known if she shared them with anyone and if she did, with whom.

The reason for such a request was a critical article about her published last November in Weekly magazine with the headline "Robbery of Serbia - how are all involved connected" with the subtitle dedicated to her titled "Who returned the queen of privatisation to the scene of the crime?". The article quotes an email from one of the employees notifying some institutions that the Agency management has banned all work meetings, and disallowed them from communicating via email.

The acting IT manager in the Agency at the time stated that the published article was the key reason behind the General Manager's intent "to prove leakage of information from the Agency", while in fact she wanted to find out who told reporters about her bad business management of the Agency. According to oral accounts, the IT manager consulted with his solicitor regarding the legality of copying emails without the employees' consent. The solicitor told him that such an order is not in accordance with the Law on Personal Data

Protection and the Criminal Law. In fact, his lawyer informed him that the penalties for unauthorised processing of data and breach of confidentiality, range from RSD 50,000 to 1,000,000, but can also mean imprisonment of up to two years.

The IT Manager stated that when he asked the General Manager why she would need copies he was told that this was no concern of his. He also said that persons not employed or engaged, nor having formal relations with the Agency, were present at the meetings related to this issue.

In a reply to the media, the General Manager of the Agency said that she had never asked for emails to be copied, and she denied that any employee email was copied. Asked whether the IT manager was fired because of his opposition to this act, she replied that he had been dismissed for not doing the work according to his contract but did not go into further details. The former General Manager highlights that she was unaware of the magazine article about her and that she had just retired from the position of General Manager of the Agency a few days earlier.

It is not known what measures have been undertaken to close the gap in the Agency security system, as it was through a formal chain of command that the Agency IT system was abused. The best conclusion to draw from this case is that lack of ethics and IT corruption related training and awareness for civil servants could be a big problem as they are important as crucial long-term safeguards against IT-related corruption.

Serbia case 4: "Road mafia"

The trial for "Road mafia" in Serbia that begun in May 2007 involved 53 persons, mostly employees of the state owned company Serbia Roads ("Putevi Srbije"), who electronically diverted road tolls. It was described as the largest electronic robbery in the history of Serbia's judiciary[36].

In November 2009, the Belgrade District Court Special Department sentenced 41 persons to a total of 131 years and 10 months in prison. The defendants were found guilty of withholding part of the money collected from road tolls, robbing Serbia's public road company "Serbia Roads" of some 6.5 million euros in the process. Nine of the accused were acquitted, while three committed suicide during the trial proceedings[37]. Milan Jovetic, who was employed with

36 http://www.setimes.com/cocoon/setimes/xhtml/en_GB/newsbriefs/setimes/newsbriefs/2007/05/29/nb-06

37 http://www.balkaninsight.com/en/article/serbia-s-road-mafia-get-131-years The outcome of Appellate Court second instance verdict were slightly lower sentences.

Serbia Road's internal control, and who was marked as the group's organiser, got the highest jail term of six years. The second accused, Zivorad Djordjevic, who is also believed to be one of the group leaders, received three years and two months in prison[38].

In Serbian public discourse it is quite common to suspect that people accused and sentenced for corruption offences are often only a little bit more then "scapegoats", since the high-level corruption cannot function without either active involvement or "silent approval" from the political level. However, it is rather unique for such a scenario to be almost entirely confirmed by the judicial bodies:

"The Court considers that Jovetic and Djordjevic are not real organisers of the group and that the actual organisers, unfortunately, remained unknown. We have evidence... that some other people are guilty ... It remains unknown who was the organiser in Belgrade and who was taking 40 per cent of the money"[39].

One sentenced worker from "Micros Electronics", as the verdict reads, "designed and developed the mechanisms and technical means that enabled illegal work and collection of money", by "using connecting cables, existing electronic devices and a special, irregular software program". One set of cables connected the upper and lower printer on the ticket distribution machine. Another set of cables, with a switch, connected (or disconnected) the car entrance ramp and computer on the toll station. This mechanism was installed on "Bubanj Potok" and "Nais" toll station (two ends of the Belgrade – Nis highway). He also inserted a corrupt copy of the software file "EMU-87", in the existing operative system for toll collection. That enabled, without changing the electronic system, registration of toll payment receipts. The shift supervisors started the illegal program before selected collectors began their shifts.

Regular software, including the original file "EMU 87" served as a mathematic coprocessor for arithmetic operations. As old computers did not have such a coprocessor, the EMU 87 file originally served only to "emulate" it. Since that file was a part of the original system, the maintenance worker just overrode the original file with the illegal one. Differences between the original and fake EMU 87 could be observed when opening the file in a text editor. While the original file has "some hooks and handles" to make it unreadable, the illegal file contained an easily readable form of receipt that stated the road toll was collected. The system made it possible to see properties of the file, dates of access, etc. As one of the controllers explained, checking and auditing did not identify the fraud, as it did not leave any traces in the system.

38 Ibid.

39 Judge Vladimir Vucinic, according to "Politika" daily, http://www.balkaninsight.com/en/article/serbia-s-road-mafia-get-131-years.

The combination of cables, special electronic devices and illegal software enabled toll collectors (members of the gang) to simultaneously print two copies of a highway toll ticket with identical serial numbers, while the electronic system registered only one. When the toll, on the basis of the first doubled ticket, was paid, the software enabled printing of a receipt without registering it in the electronic system for payment collection. At the same time, by pressing the switch, it was possible to let trucks continue their trip after the payment, since such switching interrupted connection between the system for electronic control of payments, the computer, and the road ramp. The same worker of Micros Electronics, who installed the illegal file, also maintained the illegal system when necessary (changing cables, hiding the illegal software when necessary, educating others how to use the system, etc.).

The reason why the system could operate for so long was the lack of effective control and how widespread the criminal network really was. Members of the gang did not even remove illegal cables after their shifts, the shift chiefs did not warn them of doing so, and illegally gained money was usually kept in the cabins where it was collected. Control was performed usually after 6 PM (when the gang did not operate), and there were codes for advance warning of intended control, etc.

It is an interesting fact, mentioned in the court verdict but not further elaborated on, that in the period covered by the verdict (between 2004 and 2006) the overall sum of collected highway toll money effectively increased, while the opposite should have been expected as a consequence of the theft. This, however, is a strong indication that the fraud system functioned during a much longer period of time, and that the investigation covered only some of its aspects and perpetrators.

The "road mafia" case was the first to enlighten the public into one of Serbia's best known whistle-blowers[40], a man who was a temporary employee of the "Serbia Roads" company. When he started to speak about the problems with other colleagues, the reaction was to allow his contract to expire in early 2006, and with a "lack of need for such services" given as an explanation.

"Then, I decided to prove suspicions of stealing on toll stations, the issue that nobody wanted to raise, being afraid of being fired. I secretly taped tracks passing Nis and Belgrade toll station, including the tickets. However, in order to prove the case, I needed the official listing of tickets, so I could demonstrate that there were duplicates", he says.

40 Serbia still does not have a law that would enable effective whistle-blower protection.

The whistle-blower taped the ticket a truck driver received, including the communication with drivers. Then, he needed the official listing. However, "Serbia Roads" rejected free access to information requests. The Commissioner for Information has spoken several times in public about this case. When the whistleblower asked for his help in order to receive the listing of toll payment slips distribution, the Commissioner asked "Serbia Roads" to explain the reasons why they denied the requested information. The Commissioner did not accept the argument that it was a commercial secret, and he passed the order to make the listing public.

"My decision was binding for 'Serbia Roads' under the law, but they did not act according to it. The Serbian Government, which must provide enforcement of the Commissioner's decisions if necessary, did not do it."

The man who brought this issue to the public's attention also testified as a witness in the trial that followed. It is interesting that his tape, one of the pieces of potential evidence of criminal enterprise, disappeared from the court files before the main hearing.

2. Safeguards against abuse of IT

Introduction

By Louise Thomasen

The case examples in chapter 1 concern a variety of Information and Communication Technology (ICT) abuses and corruption offences. In order to learn from the cases both what safeguards were missing and how the countries have learnt from the case examples, national authors will in this chapter describe both specific and general safeguards against ICT corruption for their respective countries.

Specific safeguards against Information Technology (IT) corruption are:

- Technical safeguards against unauthorised access and abuse of ICT systems
- Organisational and procedural safeguards such as the 'many eyes principle'
- Monitoring data traffic and employee access to data systems
- Training and awareness measures for civil servants on risks of ICT corruption and safeguards
- Auditing of ICT systems (internal or external audits; initiated by the state body, or by reports or complaints from citizens or the press)
- Legislative safeguards, such as comprehensive administrative, civil, and criminal legislation to prevent and sanction abuse of ICT for corruption

As the cases are describing abuse of ICT for corruption that has already taken place, we have not looked for examples that had any specific outcomes resulting in additional or planned safeguards. The cases in chapter 1 are real-life corruption cases, and as such will supplement and enrich what we can learn about what safeguards there should be in place to fight corruption that uses ICT.

Some case examples may not have had any consequences, e.g. having been brought to court, and in some examples it is unclear exactly who did what, where, and how. What is important is that we can learn from the cases – learn about what safeguards should have been in place, where IT systems

are vulnerable for abuse and ICT corruption, and learn about how far the Western Balkan countries in the ReSPA network have come in realising and implementing safeguards against ICT abuse and corruption in the public sector.

Albania

By Edlira Nasi and Ened Kercini

In the information age, as we have become increasingly dependent upon complex information systems, it is surprising how little attention has been devoted to those tasked with the operation and administration of these systems. These people hold positions of unprecedented importance and trust. Malevolent actions on the part of such an insider can have grave consequences.

These cases demonstrate several points about the insider threat to the information systems. Yet it will be made clear that insider problems already exist within, including the police, military, private companies and energy sectors. Also it will be shown that there is a strong tendency for management to settle these problems quickly and quietly, avoiding adverse personal and organisational impacts and publicity.

We were unable to really prove how widespread the problems are. What is reported here appears to be only the tip of the iceberg.

Furthermore, and paradoxically, in spite of the evidenced internal issues and the particular vulnerability of public infrastructure, little is done to increase protection internally, while major investments are continually being devoted to detect and prevent external penetrations. While, protection from external threats is indeed important, human problems cannot be solved with technological solutions.

Public infrastructure information systems will remain for a long time vulnerable to misuse and abuse by those who simply know the system: the insiders.

The main issues we have noted in our cases are the failure to understand the weaknesses of the at-risk employee and the failure to have standardised rules governing the use of information systems, both with explicit consequences for misuse.

Albania case 1: Corruption in the TIMS system of the border control

This case represents a typical abuse of office and bribery of the border police officers by intentional false data entry in the TIMS IT system (Total Information Management System), with an intention to evade the payments due to the state for the use of an imported vehicle.

The main issue here is the fact that there is a great difference in how the system actually works regarding tracking people when border crossing, and how it was designed to track vehicle registration numbers.

Advances in recent years on identity documents and dedicated reading devices installed at all cross border points, have greatly improved the process of people registration, improving automated data capture quality, thus making it easy and transparent by reading biometric identity documents information stored electronically inside a RFID enabled secure chip.

The same thing cannot be said about tracking vehicle registration numbers. This is still a manual process involving human work in reading appropriate documentation, verifying the authenticity of information, and also cross-checking it with unique numbers buried deep in well-known specific places within a vehicle.

It is this system's vulnerability that was successfully exploited by an insider who was able to produce an 'original' document based on false information keyed into the TIMS System. We need to emphasise that, in fact, the information was true; it is only the time stamp which was falsified. A much greater issue (beyond the scope of this study) is the fact that the vehicle passed through customs in late 2009 without proper registration procedures at all.

In this case, no special or sophisticated IT tools were used, as it was simply an intentional information system misuse; IT was first initiated by not registering the car in the TIMS system when it initially entered the country, and then a repeated misuse was made when - after 4 years - the owner finally wanted to register the car.

The TIMS information system has very good user levels privileges and administration. Regulation and procedures were followed appropriately by

border police forces maintaining information and respective signatures in the traditional paper based logs books. The TIMS also has a proven built in capability to log and track who did what, and it was thus easy to spot the 'insider' once indications were received and confirmed by other collected evidence. As such the TIMS system has proven its capabilities to support the auditing process.

We could not confirm that this case initiated a system improvement; however this does not exclude many system software improvements, software fixes and other procedural changes that are applied periodically. CCTV monitoring and recording was considered and successfully applied as a good deterrent to minimise rules violations and help the authorities identify the wrongdoings in case of investigations.

Albania case 2: Corruption in the Electronic Public Procurement System

The case concerns stealing user identity to secure privileges of the public procurement system with clear intention of deforming the final decision of procurement process.

Albania has had an electronic procurement system for many years, and it is considered a successful project. The system has impacted positively on the overall costs of government expenses procuring goods or services.

In short, the system permits the publication of tender documents. Bidders can then upload their documents in the system and submit their financial offer. The process is encrypted. It remains encrypted until the bidding deadline is reached, and it can only be decrypted if at least three or more previously authorised officials enter their 'usernames' and 'passwords' within a well-defined timeframe. In some ways this secures a good level of bidding transparency. The procurement system is also able to sort and automatically collect and notify bidders in full compliance with the procurement law, by-laws, and directives. It is important to note that it is becoming good practice that before the Supreme State Audit conduct an audit of a public entity, they usually get a complete detailed report from the public procurement system regarding the entity and time period they plan to audit.

What triggered this case was that the Supreme State Audit was able to identify a discrepancy between information collected by the electronic system of public procurement and the paper based tender documentation signed by the appointed tender committee.

How could this happen? Initially when the bidding committee starts the tender procedure they enter a dedicated area of the electronic procurement system. Similar to a self-service application, after the initial setup, each member can enter his 'username' and choose a 'password'.

This system offers fail back functionality in case somebody needs to reset his password. This feature can be activated by the appointed head of the bidding committee. It will send an email back with a reset link to the original users email box, as every user must have an email address registered to be enrolled in the system. That seems ok, but in fact lowers security to the level of the user's email password, as in general all users are registered with an official email address which is sometimes shared or to which people know the password. This means that in reality they all know each others 'passwords'. Although this practice was implemented with the good intentions of solving working issues, it reduces system security overall.

We have also identified another interesting issue. Even when procedures and regulations were put in place and were enforced by information system capabilities like accepting only strong passwords and asking periodically for password change, another human factor begins to appear - greater 'ease of use'. We have seen the data that confirms it. The majority of users become annoyed, especially with periodically changing complex passwords, and take the shortcut to leave passwords unchanged with the default value that the system admin initially supplied them for first time log-in. After three months their accounts are blocked, but it is much easier asking for a password reset to the same initial default value the system admin always supplies. In the end, almost all email passwords will be similar.

It was quite impossible to prove what happens and no log-files were available to further trace this issue deeper. In the eyes of the Supreme State Audit, the only thing certain was that the member of the tender committee could prove that he was not even in Albania.

In the end, good system design and procedures will fail, a chain is only as strong as its weakest link and in this case we strongly believe that it really was too easy to impersonate a user identity by knowing this email password weakness and exploiting the procurement system password reset facility.

We do think that there is no way to ensure proper security and protection using only passwords. The new system must be updated with capability to use two-factor authentication, which at least could leave no room for abstract and silly evading arguments for users' identities.

Albania case 3: IT corruption in the power distribution operator

This case represents a high profile information system's 'insider' manipulation; the system was programmed to provide systematic value changes to levels of consumption within the billing system. This allowed the manipulator to increase the values of energy bills with the intention of gaining financial benefits for the company.

This case also represented the greatest difficulties for information gathering because of the expertise used in managing it internally from the private company, the high monetary values involved, and the greater attention of the displeased public.

We do not have, in this case, the usual data which would provide enough information to understand what really happened with the information system. However, we were able to make sufficient assumptions based on the hard facts that were collected at the time.

There is a loop in PDA metering data that based on certain indicators can be filtered and are not sent directly to the billing, as it may present problematic clients, fines and other unusual billing issues that need to be further reviewed by staff. It makes sense that this data was filtered under consideration of previous payment issues, or where those tasked with metering had suspicions that consumers were tampering with their energy consumption. The fact that the metering process was executed, according to the logs, during the late hours and beyond the daily working hours of the metering staff, could be a key indicator that the overbilling was intentional and abusive.

The timestamp of the transaction is very suspicious and it was one of the main alerts during the investigation. Field PDA operators had not only violated protocol on the timing of gathering data, but the timestamps indicate frequencies of use that are not humanely possible. Thus, there was either data manipulation or fictive gathering of data. The analysis of the data indicated to the latter.

It could also be considered a sophisticated attempt to potentially execute a fraud on almost 15,000 consumers. Again the same pattern can be identified, intentional information system misuse - this time for increasing company profits. The difference is that this operation cannot be the work of a single person, and there is a need for approval privileges to execute such an operation, and as the profits go directly to the company finances, nothing remains to support justifications like billing system error or a mistake by staff.

Albania case 4: Embezzlement and forgery in bookkeeping

This case, looking quite innocuous, represents a very distinct system misuse by an employee responsible for bookkeeping, who throughout the years embezzled funds she was appointed to administer.

The key to better understanding why this is interesting is that it does not really involve the information technology used but the exploitation, on the part of the treasurer, of the lack of oversight or attention shown by her supervisors.

How has this worked out? First, the financial system responsible for accepting payrolls and delivering them through the banking system seems to have been unable to simultaneously process individual details of the payroll for all public administration and other government units like the military in question. Second, there was a serious issue of trust involving internal higher management and a missing crosscheck between different signed documents for the payroll between financial authorities.

It could be that the first indication about these potential issues comes to light not intentionally, but as a result of a common error, something that could well notify the finance employee of the weakness of the system. After that, the employee intentionally inserted another mistake in the payroll to prove that the financial system was unable to properly detect the mistake, and thereby gets confirmation that the main financial check is performed on the total payroll expenses, which must not exceed a certain pre-programmed budgetary limit specified in the beginning of the fiscal year.

The only thing remaining to be figured out is that for such a scheme to work it needed a perfect adjustment between several payroll paper-based documents. These payrolls need only remain with the same total sum at the end of the month. Thus tables could be easily manipulated as long as individual details are kept within what the treasury's system anticipates as the total amount so as not to arouse any suspicion. At the same time there will be minor negative differences for most of the individuals' payrolls that can be summed up to a one single account which includes a final sum. That was possible because the banks are usually not interested in what a person's individual payroll value is. What is important is that the number that was disbursed by the treasury adds up as the total of all payrolls. The various components and ranges that military payroll has, such as benefits and other additions, makes it even harder for treasury staff and the bank to become suspicious of anything that may seem to be beyond the normal payroll rates.

This is the reason why the embezzlement was possible for a prolonged period of time. As long as the total sum did not exceed the sum approved by the Chief of Staff and the Commander, the scheme could continue.

This kind of system misuse could be described as a man in the middle attack. An attack in this case was performed by someone within the system who was trusted by his or her superiors, who confirmed payroll without reviewing it further, and exploited the interesting fact that between the treasury and the bank only the total sum of all payrolls was exchanged.

Actually this kind of loophole is now closed, as the treasury software has been modernised and data exchange with banks now contains more details from the treasury system.

IT corruption measures in Albania

Legal Safeguards

As far as legislative safeguards are concerned, Albania has recently reviewed its legislative framework and its Penal Code in order to reflect the emergence of cybercrimes or IT related crimes. The most relevant ones that also are related to the field of abuse of databases or IT resources Law no. 10023, dated 27.11.2008 "On some additions and changes in Law no. 7895, dated 27.1.1995 "Code of the Republic of Albania", as amended, added new offences to the Penal Code, including computer fraud[41], computer falsification[42], unauthorised computer access[43], unlawful wiring of computer

41 Article -143/b - Computer fraud - "Entering, modifying, deleting or omitting computer data or interfering in the operation of a computer system, in order to ensure for oneself or for their parties, through fraud, an unfair economic benefit or to cause to a third party asset reduction, are punishable by imprisonment from six months up to six years. This very act, when committed with accomplices, or more than once, or when it brought about serious material consequences, is punished by imprisonment from five to fifteen years."

42 Article 186/a - Computer falsification - "Entering, modifying, deleting or omitting computer data, unlawfully, in order to create false data aiming to submit and use them as authentic, despite of whether the created data are directly readable or understandable are punishable by imprisonment from six months to six years. When this very act is committed by the person whose task is to safeguard and administrate computer data, with accomplices, more than once, or has brought about serious consequence to the public interest, is punishable by imprisonment from three up to ten years."

43 Article 192/b - Unauthorized computer access - "Unauthorized access or access in excess of the authorization to access a computer system or in a part thereof, through violation of the security measures, is punishable by fine or imprisonment up to three years. When this very act is committed in military, national security, public order, civil protection, health computer systems or any other computer system of public importance, it is punishable by imprisonment from three up to ten years."

data[44], interference in computer data[45], interference in computer systems[46], as well as misuse of equipment[47].

Furthermore, legislation covering electronic databases has been adopted recently, responding to the need for a legal basis pertaining to the creation of electronic databases in order to improve public services; these legal acts also have implications for the use and management of database information and procedures to be followed by employees in order to achieve the required standards of the law regarding the security of the data. Law no. 10 325 dated 23.09.2010 "On state databases" prescribes the means of registration and management of state databases, while it also establishes a Responsible Coordinating Authority, regarding the regulation of databases and their use.

The Minister of Innovation and Information and Communication Technology (now the Minister of State for Innovation and Public Administration) has proposed to the Council of Ministers specific measures to ensure the security of databases. Specifically, Decision of the Council of Ministers no. 961 dated 24.11.2012 establishes as Responsible Coordinating Authority the National Agency for Information Society while Decision of the Council of Ministers no. 945 dated 02.11.2012 approves the regulation on the administration of databases. An important aspect of this regulation on the administration of databases is the specification of the levels of security, into high, medium

44 Article 293/a - Unlawful wiring of computer data - "Unlawful wiring through technical equipment of non-public transmissions of the computer data from/or within a computer system including electromagnetic emissions from one computer system that contains such computer data is punishable by imprisonment from three to seven years. When this very act is committed from/or within military, national security, public order, civil protection computer systems or in any other computer system of public importance, it is punishable by imprisonment from seven to fifteen years."

45 Article 293/b - Interference in computer data - "Unauthorized damaging, distorting, modifying, deleting or suppressing of computer data is punishable with imprisonment from six months to three years. When this very act is committed on military, national security, public order, civil protection, health computer data or on any other computer data of public importance, it is punishable by imprisonment from three to ten years."

46 Article 293/c - Interference in computer systems - "Creating serious and unauthorized obstacles in order to harm the operation of a computer system, through entering, damaging, distorting, modifying, deleting or suppressing the data is punishable by imprisonment from three to seven years. When this very act is carried out in military, national security, public order, civil protection, health computer systems or in any other computer system of public importance it is punishable by imprisonment from five to fifteen years."

47 Article 293/ç - Misuse of equipment - "Manufacturing, keeping, giving for use, disseminating or any other action to place at disposal an equipment including a computer software, computer password, access code or another similar data that have been created or adjusted to access a computer system or a part thereof, aiming to commit a criminal offence envisaged by articles 192/b, 293/a, 293/b and 293/c of this Code is punishable by imprisonment from six months to five years."

and low[48], where the level of security is specified based on the parameters of integrity, confidentiality and availability of data[49]. Technical security measures are then taken on the basis of the categorisation of the databases. Security measures to be taken are overseen by the National Computer Security Agency. However, as the National Computer Security Agency is a rather new institution with very limited human resources, it is in the process of increasing its capacities in order to fulfill the requirements attributed to it by law.

Other relevant laws with regard to IT issues include the following laws and documents which ensure the proper implementation and use of IT systems:

- Law no. 9880, dated 25.02.2008 "On electronic signatures"
- Law no. 9887, dated 10.03.2008, as amended by Law no. 48/2012 "On the protection of personal data"
- Crosscutting strategy for the Information Society 2008-2013
- Law no. 72/2012, "On the organization and functioning of the national infrastructure of geospatial information in the Republic of Albania"
- Law no. 9918, dated 19.05.2008 (as amended) "On electronic communications in the Republic of Albania"
- Law no. 119/2014 "On the right to information". (voted in late September 2014 and replacing Law no. 8503, dated 30.06.1999 "On the right to information on official documents")

Technical corruption safeguards

With less concern for people, a major part of information systems security strategies are technical in nature. Two main governmental agencies in Albania NAIS (National Agency on Information Society) and NACS (National Agency on Cyber Security) with the help of ASPA (Albanian School of Public Administration) are involved in training information technology staff to better protect government systems against possible corruption abuse. The role of the National Computer Security Agency is especially important, if we consider that it would be the institution to provide expertise on the auditing of security and other measures of the databases. The specificities of the auditing of databases provide an interesting backdrop to better understanding how IT safeguards are put in place. According to the regulation on the administration of state databases, systems are audited regularly, every two years for high security databases, every three years for medium security ones and every four years for low security databases. The process followed ensures that technical safeguards are in place, as the Regulation provides that auditing should

48 Article 17, DCM no. 945 dated 2.11.2012 (Annex 1)
49 Ibid, Article 18

include the verification of the compliance with the inventory of system assets, the control of whether security measures are adequate, as well as control over whether technical measures and security measures are adequately implemented[50]. Based on the reports and minutes of the auditing, institutions are to take adequate steps to rectify any non-compliances evidenced.

Organisational and procedural safeguards

A procedure regulated by law is now implemented (Instruction no. 2 dated 9 February 2013 of the Minister for ICT "To standardise the development of Terms of Reference for ICT projects in the public administration"), whereupon every government entity that revises or builds an information system must get both a design review, and receive no objection to the terms of reference from the experts in the National Agency for Information Society. This is an Albanian strategy for utilising the best local expertise and know-how, from initial public IT project conception to the finalised tender documents.

The new Albanian government, with an agenda of fighting corruption, has recently introduced a new procedure with the support from the National Agency for Information Society related to the information systems acceptances. It is expected to have a different approach when information systems are accepted, opening the participation on that working group assigned to do the acceptance with external experts. It is hoped that this could greatly reduce some issues that were previously found with information systems projects during the acceptance period (to many tolerances and many uncompleted works) mostly connected with technical staff and management staff.

To say that security is something that can be easily purchased is an incorrect allegation; the human factor can demonstrate that the most reliable expectations are incorrect.

Training and awareness

Albania has another ongoing initiative coming from the 'National Agency on Cyber Security' in cooperation with the 'Albanian School of Public Administration' organising training courses for almost all information technology staff in public institutions and other government entities. The training courses vary amongst different themes such as systems security, protection, and external and internal risk evaluation. This could be the first sign of a positive development changing focus from equipment and software to the people who administer and use them.

50 Article 24 (3), Decision of the Council of Ministers no. 945 dated 02.11.2012

Conclusion

As a conclusion, we feel confident that it is necessary to investigate other ways of managing information systems security and preventing corruption from within the system as they usually tend to disregard the social factors of risks from 'insider threat' and the difficulties to adjust information processes with informal structures of public institutions.

Bosnia and Herzegovina

By Aleksandra Martinovic and Srdjan Nogo

Introduction to examples of safeguards against abuse of IT

When IT tools are harming the reputation of individuals or institutions, then using these tools and technologies is becoming a form of criminal offence. In many cases, cyber-crime activities in BiH are very difficult to prove and legal consequences and penalties for such activities are weak. In order to prevent such criminal activities, Bosnia and Herzegovina has already taken steps in the fight against cyber crime, through the implementation of the following projects:

- a centralised identification protection system of citizens (IDDEEA),
- a PKI infrastructure (Electronic Signature Act BiH),
- a centralised umbrella system of e-Government projects for exchange of information between all levels of governments in BiH,
- Public Administration Reform Office (PARCO) projects for the improvement of public administration.

There are also many other activities and projects, implemented through Europe Aid and other bilateral funds, which are significantly helping in the fight against corruption.

Bosnia and Herzegovina signed the "e-SEE Agenda for the Information Society" in 2002 in Belgrade, and became a member of the Electronic South Eastern Europe. In the agenda, it was agreed that state parties have to develop and adopt a policy and strategy for development of SEE information society, and a "Single SEE Information Space – Priority Area", which defines a way of establishing a public infrastructure for safe operations based on a qualified electronic signature.

The “Law on Electronic Signatures” and the “Law on Electronic Legal and Business Transport” were adopted in 2006. Decisions governing the field use of electronic signatures and certifications were also adopted to ensure the necessary legal framework for implementing digital signature.

Safeguards in Bosnia and Herzegovina case examples

This is a case concerning a State prosecutor who was alleged to have hacked the email account of the former General Prosecutor, in order to discredit him, just prior to his suspension from official duty as a General prosecutor.

Technical safeguards against unauthorised access and abuse of IT systems

The responsible persons from the BiH judiciary have learnt that the existing security measures were not enough to prevent intentional illegal access to a computer system - namely, an official mail account of an employee. The BiH judiciary therefore improved security procedures at all levels and implemented standard ISO / IEC 27001:2005.

Organisational and procedural safeguards such as the ’many eyes principle’

Although everything was implemented according to the law, procedural safeguard measures that were already in place were insufficient and inadequate to prevent human factor error and weak security awareness of people using the IT infrastructural system.

Monitoring data traffic and employee access to data systems

Laws and procedures of the BiH judiciary prescribe monitoring of data traffic and monitoring of employee access to data systems. According to internal reports, made by various judicial institutions, it was recognised as a necessary precaution, and as such is used to safeguard against corruption and cyber crime.

Training and awareness measures for civil servants on risks of IT corruption and safeguards

Yes, the Agency for Civil Servants of Bosnia and Herzegovina and similar entity level agencies, have been training their civil servants to reduce the

risk of conflict of interests arising, and to enhance a code of conduct in public administration in all governmental administrative levels.

The Agency for the Prevention of Corruption and Coordination of the Fight against Corruption is a state level institution, which is also in charge of the development and monitoring of the educational training on prevention and fight against various forms of corruption. Due to the lack of political will to fully staff and equip the Agency, it has lacked capacities to fully implement all tasks prescribed by the relevant laws.

Auditing of IT systems

The organisation now implements additional auditing of IT systems so as to prevent abuse of IT system in the future.

Legislative safeguards

- Law on Electronic Signature
- Law on Electronic Business
- Law on Electronic Legal and Business Transport
- Law on Protection of Classified Information

Bosnia and Herzegovina case 2: Another possible controversial employment in Supreme Audit Institution of the Republic of Srpska

The case of a written test to select two junior performance auditors for the Supreme Audit Institution of the Republic of Srpska, where data from the test has gone missing, and where there is a possibility that one candidate has already been selected before test results have been published.

Technical safeguards against unauthorised access and abuse of IT systems

As for the security measures (technical safeguards) to prevent these kinds of problems in the future, according to sources within the SAI RS nothing has been done so far.

Organisational and procedural safeguards such as the 'many eyes principle'

Not only were there areas which had not been properly implemented according to the law, even some of the procedural safeguard measures that were in place were insufficient and inadequate. Candidates should take the tests using safe software, but instead candidates wrote their tests in a simple word format without any protection, so that any person from the responsible commission had an opportunity to make changes to the tests. Furthermore, this time candidates were not allowed to make copies of the tests to their USB memory sticks and the tests were not given to them for review.

Monitoring data traffic and employee access to data systems

The organisation has not learned anything from this case and there is no awareness that monitoring data traffic is necessary as a safeguard.

Training and awareness measures for civil servants on risks of IT corruption and safeguards

Yes, the Agency for Civil Servants of the Republic of Srpska, has been training its civil servants to reduce the risk of conflicts of interest, and to enhance code of conduct in public administration in all governmental administrative levels.

Auditing of IT systems

The organisation should implement internal auditing of IT systems and it is their obligation under the Law.

Legislative safeguards

N/A.

Bosnia and Herzegovina case 3: Misuse of CIPS project's electronic system

The Citizen Identification Protection System (CIPS) project started in Bosnia and Herzegovina in April 2002, when, on a temporary basis, the directorate for its implementation was established. The main task of the project was to

establish a part of the system through which the Law on Central Registers and Data Exchange would be implemented. From the very early stages of the CIPS project, a number of complaints were recorded about the misuse of its electronic system, particularly when issuing personal identity cards and passports throughout the country.

Technical safeguards against unauthorised access and abuse of IT systems

Between 2012 and 2015, IDDEEA implemented the following standards: ISO/27001:2005 and ISO/90001:2008 (with their scheduled audits[51]).

IDDEEA's DMS (Document Management System) used for keeping data on state and entity level institutions as well as agencies whose requirements are to be compliant with a very high standard of IT safety and security.

Organisational and procedural safeguards such as the 'many eyes principle'

- To proceed with implementing more relevant standards and to use audit service regularly according to EU rules and legislation with a special look at ISO 9001 Quality Management standards.
- Employee security check implemented at the competent authority (Intelligence and Security Agency of BiH) which ensures avoidance of IT security breaches and also collects personal data of all contracted personnel in order to make a social profile for future use.

Monitoring data traffic and employee access to data systems In terms of infrastructure, data transmission security institutions in BiH have established a highly sophisticated communications network through Synchronous Digital Hierarchy (SDH) technology that enables fast, reliable and efficient sharing of data, images and sound. The SDH network is a closed system, not connected to the Internet and works on a specific range of frequencies covered for that purpose. The institution that maintains the technical SDH network, the Agency for Identification Documents, Registers and Data Exchange (IDDEEA), is in charge of the identification documents, storage, personalisation and transport of documents, as well as central record keeping and exchange of information between the competent authorities in Bosnia and Herzegovina.

51 http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=415&Itemid=214&lang=en

IDDEEA[52] monitor, coordinate and regulate the institutional field of identification documents, and as such has developed an electronic signature in a closed system – and its experience on the application of electronic signatures in closed systems is very important for the implementation of the Law on Electronic Signature BiH and open systems.

The **key problems** are:

- Lack of institutional arrangements necessary to coordinate activities in the field of e-Government services (performed by different levels and different ministries),
- Irrational use of (inadequately distributed) IT personnel,
- Inadequate ICT policy and legal frameworks in use by government authorities at state and entity levels, and
- Failure to implement IDDEEA guidelines.

Training and awareness measures for civil servants on risks of IT corruption and safeguards

Agency for civil servants of BiH and similar entity level agencies have been training its civil servants to reduce the risks of conflicts of interest, and to enhance code of conduct in public administration at all governmental administrative levels.

IDDEEA has implemented an e-Learning platform for continuous education and skill improvement of its personnel which is necessary to achieve the highest standards of effectiveness and professionalism.

The Agency for the Prevention of Corruption and Coordination of the Fight against Corruption is a state level institution, which is also in charge of the development and monitoring of the educational training on prevention and fight against various forms of corruption. Due to the lack of political will to fully staff and equip the Agency, it has lacked capacities to fully implement all tasks prescribed by the relevant laws.

Auditing of IT systems

Yes, the internal audit department for IT information system was established to prevent abuse of IT systems.

52 http://www.iddeea.gov.ba/images/stories/PDF/law_on_agency_final.pdf

Legislative safeguards

- Law on protection of persons who report corruption in the institutions of Bosnia and Herzegovina ("Official Gazette of Bosnia and Herzegovina" no. 100/13)
- Law on Administration ("Official Gazette of Bosnia and Herzegovina" no. 32/02 and 102/09),
- "Guidelines" on filing internal reports of suspicions or concerns about corruption by employees of the Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina, 31 March 2014.

IT corruption measures in Bosnia and Herzegovina Fight against corruption

All relevant domestic and international reports on the state of corruption in BiH are pointing out that corruption is among the biggest problems in society and the major obstacle to various reforms and overall economic and social progress. The latest EU progress report on BiH indicates once again that the country is at an early stage in the fight against corruption[53]. Furthermore, key pieces of anti-corruption legislation have been amended in ways that undermine previous achievements. Corruption remains widespread, with an insufficient track record of investigation and prosecution in high-profile cases.

Judicial system

In 2013 the High Judicial and Prosecutorial Council (HJPC) took a series of measures and concrete actions that should contribute to more professional and better quality work by prosecutors. Case 1, described in chapter 1, as we believe, contributed to the rapid automation and professionalisation of this system. Knowledge, skills and understanding of current issues, of the importance for the prosecutorial work, were increased through a special engagement of the project "Strengthening the capacity of prosecutors in the criminal justice system" in the area of education. These goals are achieved by developing training modules, the organisation of a number of education strategies, cooperation with JPTCs (Judicial and Prosecutorial Training Centres) in order to improve the current model used for educating prosecutors, and managing networks of all the stakeholders of criminal investigation into the educational process. In this process more than 150 prosecutors advance their knowledge in the following areas:

- criminal proceedings against legal persons,

53 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf

- witness immunity,
- study and research skills,
- special investigations,
- cybercrime,
- money laundering and financial investigations,
- trafficking, and
- communication skills and methodologies.

For the above, we noted a lot of relevant facts concerning the legislation and showed that respect for the legal framework can largely prevent this type of crime and corruption.

In addition to regular audits, during 2013, the Supreme Audit Office of BiH (SAI BiH) conducted a performance audit: "Telecommunication solutions in the institutions of Bosnia and Herzegovina". The related audit report highlighted positive examples of the HJPC, which spent a significantly smaller amount for internet services, compared to other institutions from the audited sample, although HJPC has a significantly larger number of users.

Enhanced security of the BiH judicial information system continue to be one of its strategic priorities, as indicated in the Strategy for reform of judicial system in BiH 2014-2018[54]. There are also HJCP recommendations that judicial capital investments should include replacement of outdated, and procurement of missing computer equipment; further development of information systems in the judicial system; the maintenance of the existing equipment and software licenses; and training of IT and other staff of the judiciary.

Within the process, computerisation of the judiciary, a system for the electronic exchange of data between police agencies and prosecutors' offices, was established and officially started in June 2013. Prosecutors in prosecutors' offices across the country now have the possibility to monitor electronic records under the jurisdiction of police agencies, in accordance with the valid legal framework. In addition, police agencies have the ability to track the status of police reports on crimes, filed to prosecutors' offices, stored in their system for automatic management of the cases (TCMS). The system was established under the Agreement concluded between the HJPC, the Ministry of Security of BiH, the State Investigation and Protection Agency, the Border Police, and the Ministries of the Interior at all levels of government. Support to the Judiciary of Bosnia and Herzegovina (IPA 2009) and the IPA project "Support to the Police Reform" were the two main projects that led to this system.

54 http://www.mpr.gov.ba/aktuelnosti/propisi/konsultacije/SRSP%20u%20BiH.pdf

In order to respond to the growing needs of the system, particularly with regards to a new automatic case management system for courts and prosecutors' offices (CMS/TCMS) and to ensure software solutions compatible with current software standards, the process of upgrading all hardware and software components of the ICT system (optimisation and consolidation of the ICT system in BiH judiciary) was continued in 2013. This process is carried out in order to:

- Reduce, to the lowest possible level, system downtime caused by obsolescence of IT equipment and software;
- Ensure the best utilisation of existing server and network capacities in the data centres of HJPC;
- Allow for normal operations of the users in the judicial system and easy access to the electronic services of the judiciary, publicly available via the internet;
- Improve the security of data stored in databases of the judicial information system; and
- Ensure technical requirements for the smooth exchange of data with external systems are met (police, tax and other government electronic registers), which is of crucial importance for the fight against corruption and organised crime.

Within this project, staff of the HJPC Department for ICT performed a system upgrade for the management of digital identities, as well as e-mail systems in the data centres for processing and storage of data within HJPC.

All these measures are recognized by the latest EU progress report for BiH. It points out that the judicial information and communication system is fully functional. The CMS/TCMS includes over 3.4 million registered cases, and produces automated reports on judicial performances, which contribute to policy and strategic planning decisions. Access to the judicial web portal has substantially increased, as well as access to case information by parties to proceedings or their lawyers. The Judicial Documentation Centre has also registered a significant rise in online visits.

The Judicial and Prosecutorial Training Centres of the two entities provide training for the judiciary. In an effort to improve and increase capacity building, both centres are introducing distance learning[55].

The police

As confirmed in the 2013 EU Progress report on BiH, agencies and boards established under the police reform laws are still consolidating their functions[56].

55 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf
56 The Extensive Police Reform process in BiH, which started after the civil war, included the

An inter-agency monitoring team supervising the implementation of the electronic data exchange system for police and prosecutors registries has been established. Some technical aspects in the system still need to be addressed, including the fact that the directorate for coordination of police bodies still has no access to the system databases. A Europol data protection audit has been completed.

The Police Support Agency is co-located with the directorate for coordination of police bodies and completed the Rulebook on Standardisation of Police Equipment.

Amendments to the Laws on Police Officials are pending adoption at state level. The Federation of BiH, Cantons and the Brčko District have launched initiatives to align their respective laws. Amendments concern technical and operational matters such as the use of arms and police powers and enhancing personal data protection[57].

BIH law[58] recognises cybercrime as a form of criminal behaviour in which the use of computer technology and information systems is used as a tool or a target executing the criminal-legal terms with the relevant consequences.

Basic characteristics or features of cybercrime:

- Socially dangerous, unlawful conduct for which the law provides criminal sanctions;
- Specific manner and means of committing criminal acts with or through computers;
- Special object of protection, security of computer data or information system as a whole or its individual segments; and
- The intention of the perpetrator himself or another is in this way obtaining the benefit from this harm[59].

Offences related to computers and the Internet[60]:

- Computer forgery
- Computer fraud
- Child pornography
- Violations of intellectual property

---

establishment of several important institutions at the state level, such as: State Border police, Service for Foreigners' Affairs of BiH within the BiH Ministry of security, State Investigation and Protection Agency (SIPA), Directorate for coordination of police bodies of BiH, etc.

57 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf

58 Krivični zakon Federacije Bosne i Hercegovine - Član 393 do 398

59 http://www.fup.gov.ba/?p=1697 - Federal Police Administration

60 http://www.rs.cest.gov.ba/

Unauthorised access:

- Intentional illegal access to a computer system
- Making damage to computer systems and data
- Compromising confidential data

Misuse of devices:

- Deliberate unauthorised act of the production, sale, procurement or distribution
- The access devices (including computer programs)
- Computer passwords
- CODE
- Other types of access information to the commission of acts of cybercrime

Unauthorised interception of data:

- Deliberate illegal interception of data by a computer system.
- Protect the privacy of non-public transmission of computer data from monitoring and recording.

Data interference:

- Deliberate unauthorised damaging, deletion, destruction, alteration, or unusable computer data
- Insert malicious code that represents a threat to the integrity or the ability to use data and programs
- Viruses that interfere with data

There are definitely legal measures to prosecute this and similar cases connected with IT corruption, whether that is the stealing of data or "listening" to data with the purpose of sharing "heard" information with interested parties.

IT systems and internal procedures related to the Document Management System, Archive, Prosecutors cases and other relevant documents and materials including personnel working on these systems are the subject of regular inspection by the competent authority. In some institutions this is defined through internal procedures, depending on the institution's profile. In this case, the key thing is the implementation of ISO / IEC 27001:2005, to ensure that data security is satisfactory.

What to do

To proceed with implementing more relevant standards and to use audit service regularly according to EU rules and legislation, with special consideration for ISO 9001 Quality Management ISO/27001:2005 and ISO/90001:2008 standards.

To proceed with employee security checks implemented by competent authorities which ensures avoidance of IT security breaches and also collects personal data of all contracted and future contracted personnel in order to make a social profile for future use.

Fighting organised crime and terrorism

Weaknesses in the systematic gathering, analysis, and use of intelligence by law enforcement agencies hampers strategic targeting of organised crime groups and activities. There is no systematic exchange of intelligence among the law enforcement agencies for joint operational planning.

Amendments to the State Criminal Procedure Code for more effective deployment of Special Investigative Measures have been prepared, but still need to be adopted.

In the area of judicial cooperation in criminal matters, preparations for concluding a cooperation agreement with Eurojust are at an early stage, but have progressed. The assessment of the data protection legislation has been completed. Changes to the Law on Protection of Classified Information, bringing the law into line with the relevant EU standards and providing for implementation of bilateral security agreements, remain to be adopted.

Cybercrime

The European Commission Bosnia and Herzegovina 2013 Progress report states the lack of strategy and institutions to fight cybercrime and threats:

"Bosnia and Herzegovina has neither a strategy nor institutions in place to address the issue of cybercrime and cyber security threats. *An action plan to set up a Bosnia and Herzegovina Computer Emergency Response/Readiness Team (CERT) is pending adoption by the Council of Ministers. Activities to establish CERT were undertaken. Crime reports prepared by law enforcement agencies in Bosnia and Herzegovina do not refer to cybercrimes. They do not provide exact data on the number of cases, investigations or suspects. Digital forensics and other technical means of combating cybercrime at national and international level are limited and insufficient. The Directorate for Coordination of Police Bodies is designated as a 24/7 contact point in the light of the Cybercrime Convention (Budapest Convention) but the required capacity is lacking"*[61].

61 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf

Other measures

Data exchange between public bodies

With the project "Support of the judiciary of Bosnia and Herzegovina" (IPA 2009) and the IPA project "Support to the police reform" which started in 2013, with a well-framed implementation process, and according to the agreement which established a system for electronically exchanging data between police authorities and prosecutors, - concluded between HJPC, Ministry of Security of BiH, the Border Police, the State Investigation and Protection Agency (SIPA) and with the ministries of the Interior - HJCP had begun activities that will hopefully lead to a new generation of data exchange in BiH. During this process, all the aforementioned standards should be implemented and data systems ought to be "updated" in order to avoid the examples of corruption mentioned in this study. In order to do this, tools and safeguards will be implemented in this system, which include: firewalls, Intrusion Detection and Prevention Systems (IDS), Penetration Testing and Vulnerability Scanning, sensitive data transmission procedures, External System Connections procedures and rules, antivirus and pro-defence tools, remote access controls, premises entry and exit procedures and controls, data backup on remote location combining strong password protection and physical security, and permanent employee education on IT.

The Agency for Identification Documents, Registers and Data Exchange of BiH, formerly the Citizen Identification Protection System (CIPS)[62] is a very good example of safeguard and security implementation. However, while they are a very well organised Agency at State level, unfortunately misuse exists at the local authority level.

What they learned from the misuse of CIPS project's electronic system

They are implementing ISO/27001:2005 and ISO/90001:2008 between 2012 and 2015 with scheduled audits[63]. Their document management system, Civil Data Registry, and the internal environment Oracle, which is used for keeping data of all state level institutions and agencies, is very safe and secure. The problem in this case, as described in chapter 1, is that the competent authorities (Federation BiH by the cantonal Ministries of the Interior, Ministry of the Interior of the Republic of Srpska, and by the

62 www.iddeea.gov.ba

63 http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=415&Itemid=214&lang=en

competent authority, functionally acting as a state institution in the Brcko District) with strict procedures of working with data and at the same time changing, adding, deleting and updating citizens' personal data.

The competent authorities are, as defined by law, owners of their data and IDDEEA's role in this process is just to keep and secure data, and implement all known safeguards and good security practices[64]. As this is a fact, we have to apportion responsibility for such cases to police administrations in BiH and competent authorities with other similar cases if any. This means that their standards, procedures, and general way of dealing with such problems are not acceptable.

IDDEEA has provided complete security at all levels of data protection for competent police agencies and the competent authorities in Bosnia and Herzegovina. Therefore, corruption and abuse of IT technology should be sought at the level of the competent authority where the state shall ensure and improve information security.

IDDEEA implemented digital signatures for all communication channels inside the Agency and also for external use with communication towards competent authorities.

What is lacking, however, is a Computer Emergency Response / Readiness Team[65] (CERT). Although it is anticipated that an action plan for a CERT[66] will be developed, it has not yet been created.

Electronic Signature

The technical description of Public Key Infrastructure (PKI)[67] is to boost the level of security for data exchange at the state-level primary technical component. It can either be central infrastructure with a single authority for the issuance of certificates and subordinate bodies that issue certificates for electronic signatures, or independent infrastructure at level of interoperability.

In Bosnia and Herzegovina, there is no PKI for companies and individuals at the state level. However, there are a number of independent uses of PKI, especially within electronic banking and partly in the field of e-government

64 http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=105&Itemid=97&lang=en
65 http://www.msb.gov.ba/docs/Strategija_za_CERT.doc
66 http://www.us-cert.gov/
67 http://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx

operating in closed systems. Thus, the technical problem is not so much based on the absence of PKI at the state level. Rather, the problem is to bring together and merge various existing PKI and information systems. Connecting with different PKI would facilitate the process of business and work in public administration.

Security would be strengthened, as all participants in the electronic exchange of data or ordinary citizens have an identity on this system. This minimises the possibility of abuse and allows continuous monitoring of people's actions. All systems which are integrated with PKI, in effect creating one large system, considerably reduce the possibility of abuse.

Legal framework

Directive 1999/93/EC on a Community framework for electronic signatures

This Directive establishes a legal framework for electronic signatures and certification of services at European level. The aim is to facilitate the use of electronic signatures and help them to become legally recognized within the member states.

Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC

Bosnia and Herzegovina with this European Union Commission decision relies on three widely accepted product standards for electronic signatures which presuppose respect for the qualified electronic signature.

Commission Decision 2000/709/EC - November 2000

In accordance with Article 3 (4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signature, this decision outlines the criteria that Member States must take into account when determining the state of the body that will uphold the conformity assessment device for creating a secure signature.

BiH Legal framework

At the state level (BiH), the following legal acts are currently in force:

- Electronic Signature Law ("Official Gazette of BiH", no. 91/06)
- Law on Electronic Legal and Business Operations ("Official Gazette of BiH", no. 88/07)
- The Law on Administrative Procedure ("Official Gazette" no.: 29/02, 12/04, 88/07, 93/09)
- Decision on the basis of use of electronic signatures and providing verification ("Official Gazette of BiH", no. 21/09)
- Decision on e-commerce and e-government ("Official Gazette" no. 07/10)
- Decision on office operations of ministries, departments, institutions and other bodies of the Council of Ministers ("Official Gazette of BiH" no. 21/01, 29/03)
- Guidelines on preparation and maintenance of the official website of the institution of BiH (Official Gazette no. 21/09)
- Law on protection of persons who report corruption in the institutions of Bosnia and Herzegovina ("Official Gazette of Bosnia and Herzegovina" no. 100/13)
- Law on the agency for the prevention of corruption and the coordination of the fight against corruption ("Official Gazette of Bosnia and Herzegovina", December 2009).

Moreover, currently in preparation, are the following legal acts:

- Regulation of internal organisation of the Ministry of Communications and Transport (establishment of the Office of Surveillance and Accreditation)
- The High Judicial and Prosecutorial Council (HJPC) recommended to the executive authorities in BiH that the Ministry of Transport and Communications should enact appropriate bylaws and form the institutional capacities to enable the full implementation of the Law on Electronic Signature and the Law on Electronic Business in the judicial information system which is primarily reflected in the possibility of filing submissions to the court in electronic form, as well as delivery of judicial decisions electronically (verified by qualified digital certificate)[68].

68 http://www.hjpc.ba/intro/gizvjestaj/?cid=5889,2,133 http://www.ohr.int/ohr-dept/legal/laws-of-bih/police.asp

Public procurement

The Law on Public Procurement for Bosnia and Herzegovina[69], in a unique way, included all contracting authorities under EU Directive 17/2004 and Directive 18/2004. Specific EU rules on public procurement are processed through a series of detailed directives specifying the comprehensive requirements for the regulation of public procurement procedures. In Bosnia and Herzegovina, there are insufficient specific regulations that define this field in accordance with EU regulations.

The solution to overcome the shortcomings in the system of public procurement could be to allow a single body to implement the procurement process for all competent authorities. This body would possess, if they do a review on IT and corruption, unique and centralised software developed in accordance with the Law on Public Procurement for Bosnia and Herzegovina that would be concerned with the needs of all levels of government allowing it to carry out all public procurement.

Of course, a prerequisite would be the introduction of standards and to ensure the market knowledge of the employees in terms of up-to-date information and contact with vendors. This is needed to ensure that only necessary goods and services are purchased, and that such products are the best which are available.

Croatia

By Zorislav Petrovic and Ivana Andrijasevic

Main legislative framework for information security

The legislative framework for assuring information security in the public administration information systems in the Republic of Croatia relies on the following most important laws and bylaws: the Information Security Act; the Data Secrecy Act; the Act on Personal Data Protection; the Security and Intelligence System Act; the Electronic Document Act; the Electronic Signature Act; the Security Vetting Act; the Regulation on Information Security Measures; the Regulation on the Content, Form, Filling in and Handling the Security Vetting Questionnaire; and the Ordinance on the Criteria for Establishing Information Security Advisor Positions.

69 https://www.parlament.ba/sadrzaj/zakonodavstvo/usvojeni/default.aspx?id=46717&langTag=bs-BA&pril=b

The **Information Security Act** (Official Gazette, no. 79/07) establishes the notion of information security; information security measures and standards; information security areas; and competent authorities for the adoption, implementation and oversight of information security measures and standards. This Act applies to state authorities; local and regional self-government bodies and legal persons with public authority who, within their scope of work, use classified and unclassified data; as well as legal and natural persons who gain access to or handle classified and unclassified data.

The **Data Secrecy Act** (Official Gazette, no. 79/07, 86/12) establishes the notion of classified and unclassified information; degrees of secrecy; the procedure of classification and declassification; classified and unclassified information access; classified and unclassified information protection; and oversight over the implementation of this Act. It applies to state authorities; local and regional self-government bodies; legal persons with public authority; and legal and natural persons that, in accordance with this Act, gain access to or handle classified and unclassified information.

The **Act on Personal Data Protection** (Official Gazette, no. 103/03, 118/06, 41/08, 130/11, 106/12) regulates the protection of personal data regarding natural persons and the supervision of collecting, processing and use of personal data in the Republic of Croatia. Its purpose is to protect the privacy of individuals, as well as other human rights and fundamental freedoms in the collecting, processing and use of personal data.

The **Security and Intelligence System Act** of the Republic of Croatia (Official Gazette, no. 85/08, 86/12) establishes, for the purpose of systematic gathering, analysis, processing and evaluation of information relevant for national security, with the aim of detecting and preventing activities, by individuals or groups, directed against the viability, independence, integrity and sovereignty of the Republic of Croatia; aiming at the violent overthrow of the state authority structures; threatening to violate human rights and basic freedoms established by the Constitution and the legislation of the Republic of Croatia; to endanger the fundaments of the economic system of the Republic of Croatia, required for making decisions relevant to the successful achievement of national interests in the field of national security, specifically the protection of two security–intelligence agencies: the Security and Intelligence Agency (SOA) and the Military Security and Intelligence Agency (VSOA).

The **Electronic Document Act** (Official Gazette, no. 150/05) regulates the right of natural and legal persons to use an electronic document in all business operations and activities, and in proceedings conducted before

public authorities in which electronic equipment and programmes may be applied in the creation, transfer, storage and safekeeping of information in electronic form, the legal validity of an electronic document and the use and traffic of electronic documents.

The **Electronic Signature Act** (Official Gazette, no. 10/02, 80/08, 30/14) governs the right of natural and legal persons to use electronic signatures in administrative, commercial and other operations, and the rights, obligations and responsibilities of natural and legal persons associated with the providing of services to certify electronic signatures.

The **Security Vetting Act** (Official Gazette, no. 85/08, 86/12) establishes the notion, the types and degrees of security vetting, security impediments and the procedures for performing security vetting. Under this Act, vetting is the procedure whereby the competent authorities ascertain the existence of security impediments for natural and legal persons.

The **Regulation on Information Security Measures** (Official Gazette, no. 46/08) establishes the information security measures stipulated for handling classified and unclassified information. It applies to state authorities; local and regional self-government bodies; and legal persons who with public authorities, in their respective scope of work, use classified and unclassified information; as well as natural and legal persons who gain access to or handle classified and unclassified information.

The **Regulation on the Content, Form, Filling in and Handling the Security Vetting Questionnaire** (Official Gazette, no. 114/08) establishes the content, form, filling in and handling of the Security Vetting Questionnaire for individuals and legal persons.

The **Ordinance on the Criteria for Establishing Information Security Advisor Positions** (Official Gazette, no. 100/08, 30/11) determines criteria for establishing information security advisor positions.
Apart from the mentioned regulations, there are a large number of laws and bylaws that only partially address the issue of information security, such as the Act on Electronic Trade; the Criminal Code; the Act on Archive Materials; the Act on Safety and Protection; etc. Finally, it is important to note that as a member of NATO and the EU, Croatia harmonises its regulations in the field of information security with other NATO and EU member states.

Central State Authorities competent for information security

Central State Authorities competent for information security in Croatia are:

- The **Office of the National Security Council**: the central state authority responsible for information security coordinates and harmonises the adoption and implementation of information security measures and standards in the Republic of Croatia, and for the exchange of classified and unclassified information between the Republic of Croatia and foreign countries and organisations (Article 14 of the Information Security Act);
- The **Information Systems Security Bureau**: the central state authority for technical areas of information systems security in bodies and legal persons. That is: information security systems standards; information systems security accreditations; managing crypto materials used in the exchange of classified information; and coordination of prevention and response to security threats to information systems security (Article 17 of the Information Security Act); and
- **National CERT**: the national authority responsible for the prevention of and protection against computer threats to public information systems in the Republic of Croatia operating within the Croatian Academic and Research Network (CARNet) – the main internet backbone for state sectors in Croatia. Its main task is the processing of incidents on the internet; i.e. the preservation of information security in Croatia. The National CERT carries out proactive and reactive measures within its activities in order to prevent or mitigate possible damage. Users of the National CERT are all users of the Internet in the Republic of Croatia and providers of hosting services and Internet service providers (ISP)[70].

Information System Security in general

The Information Security Act defines five information security areas for which information security measures and standards are stipulated: Security Check; Physical Security; Security of Information; Information System Security; and Business Cooperation Security.

The area of information security relevant for this study is information system security. According to paragraph 1 of Article 12 of the Information Security Act, information system security "is the information security area within which information security measures and standards are determined

70 http://www.carnet.hr/ncd

for classified and unclassified information that is processed, stored or transmitted within the information system and the protection of integrity and availability of the information system in the process of planning, designing, making, using and cease of work of the information system". Furthermore, according to the same Article, "security accreditation of the information system shall be performed for the information system where classified data of CONFIDENTIAL, SECRET and TOP SECRET level are used. Persons who take part in the process referred to in paragraph 1 of this Article shall have the Certificate with the TOP SECRET level or one level higher than the highest level of classified information that is processed, stored, or transmitted in the information systems under their competence. Measures of physical protection of facilities where information systems are located shall be taken in accordance with the highest level of classified information that are processed, stored or transmitted in the said facilities". Finally, "central state authorities competent for information security shall form the registry of certified equipment and machines used in the information system of the CONFIDENTIAL, SECRET and TOP SECRET level. Registry of certified equipment and machines shall be formed on the basis of taking over the appropriate registers of international organisations or by own certifying process in accordance with international standards".

Information security measures for the area of information system security, as stipulated under the Regulation on Information Security Measures, are:

- measures for information system protection (protection of hardware, software and data storage media, management of system configuration and user's access, control of systems interconnection, etc);
- security awareness (establishment of safety rules for employees and education on safety); and
- planning emergency situations procedures (development of procedures to follow in the case of an incident; and managing business continuity).

Information system security is implemented throughout the entire information system life cycle for classified (through security accreditation) and unclassified (adjustment to HRN ISO/IEC 27001 and HRN ISO/IEC 17799 standards) systems[71].

71 Information System Security Bureau official website, available at: https://www.zsis.hr/default.aspx?id=34

Case examples of Croatian IT safeguard measures

Croatia case 1: Call doctor for votes

This is a case of a doctor extracting data from a hospital system. According to the information from the publicly available Central Register with records on personal data filing system held by the Personal Data Protection Agency, protection of personal data within a patient's personal data register (hrv. Zbirka o osobnim podacima pacijenata), which is partly in electronic and partly in paper form, is assured by the following safeguard measures: locking of documentation in bookcases, a video monitoring system, a login and user name, and a fire protection system. In this particular case, the main problem was weak data protection, including the fact that too many people had access to the database. Apparently, there was no function in the database system that recorded who the last person to download data was. It is therefore impossible to find out who downloaded the information for the mayor candidate's letters.

Croatia case 2: Confidential Croatian radio-television database on the black market

According to the Croatian Radio-Television Act, every physical and legal person in Croatia who owns a TV or radio set is obliged to pay a licence fee. HRT holds and administrates a register of HRT monthly licence payers in the Republic of Croatia. This register is not publicly available. Since it contains users personal data, such as name and surname, address, Personal Identification Number (OIB), etc., its management and usage are protected by provisions of personal data safety legislation. According to the information from the publicly available Central Register with records on personal data filling systems in Personal Data Protection Agency, the HRT register is on the server to which physical access is granted exclusively to authorised persons. Authorised users use data from the register via application by their username and passwords or certificate. Application is available by the local network and internet, by using protected data tunnels. Finally, safety copies are in the server room in the safe.

In this case, IT has been misused for the intentional copying and illegal selling of data by an employee of HRT who either had access to the register or who knew someone with access to the register. As a result, all the above mentioned technical safeguards have been breached, as well as provisions of the General rules on work and manners of HRT, according to which

employees of HRT need to work in accordance with the highest business standards and basic ethical standards, based on several values, including confidentiality and protection of data, in accordance with relevant legislation and general rules. Evidently, these standards have not been applied.

Croatia case 3: In search for veterans

This is an example of abuse of office. Obviously, somebody from one Office for Defence took data, published or gave it, or even sold it, to someone else who then published it. There might be many different motives for publishing the register, ranging from political disputes to noble motives, such as trying to increase transparency. Still, there is no doubt that the main reason that it happened was the lack of minimum security protocols involved in the procedure of dealing with the data distributed to the Offices for Defence in different Croatian cities.

Croatia case 4: With a little help from civil servants 68 Croatian passports were sold to criminals; case 5: Policeman caught while inserting forged data in the police information system; case 6: Policeman deleting traffic offences and disclosing confidential data: they accepted even roasted lamb and 20 litres of wine as a bribe!; and case 7: Accidentally caught for disclosure of confidential data on cars and their owners!

"*Secrecy, integrity, continuous availability and control of the data and information from the MUP information system usage, is implemented through a number of organisational, system and program measures and procedures as well as division of responsibility and authorisation. All users of the MUP information system are obliged to implement data protection, as prescribed by Ordinance on the protection of MUP information system based on the electronic data processing, Ordinance on safety and protection of MUP official data and other internal directives and instructions which operates activities on MUP information system data protection. Responsibilities of officer's working position define the level of data accessibility*."

Cases such as these could be prevented by monitoring data traffic and employee access to data system, as well as training and awareness measures on risks of IT corruption and safeguards. Civil servants need to become aware of the importance of keeping their passwords secret as well as of the fact that each access to database shall be monitored. The weakest link of the safeguard process is the individual with all his/her virtues and flaws.

Croatia case 8: Every year 2 million euros disappear from the tollbooths

In this case, Autocesta Rijeka Zagreb d.d. had used the internal IT systems auditing as a safeguard against IT corruption. As a follow-up to the judges' poetic acquittal in order to prevent similar cases in the future and as an IT safeguard measure, the management of HAC decided to install cameras monitoring the work of employees in tollbooths. These cameras will not capture faces of employees nor their voices, but only their working space, hands and the process of paying/collecting the toll. The total amount of this investment was 354,000 euros.

Croatia case 9: Dirty cops - policemen disclosed confidential data to weapon smugglers; and case 10: Policeman sentenced to one year in prison for allowing his friend to fish illegally

These two cases show that even precisely defined safeguards against IT corruption may fail. Namely, according to the relevant legislation on information security, the Ministry of the Interior (MUP) has prescribed various measures to protect against abuse of its information system, which contains large number of various registers[72]. According to the safety policy and the fact that some documents that prescribe safeguard measures used to protect this system from abuse are for official use only, it is impossible to list all IT safeguard measures. However, some of them could be recognised from the available documentation and from the media releases, such as:

- **Technical safeguards against unauthorised access and abuse of IT systems**. This safeguard represents the most common threat in a networked system. The first line of defence against unauthorised access and abuse of IT systems are passwords. "*Every*

72 The list of all MUP registers are available at the following link: https://registar.azop.hr/index.php?action=search_results&query=ministarstvo+unutarnjih+poslova&cl_p=1&cl_n=10&cl_n=200&cl_p=1

policeman has his/her own password which allows him/her to access various databases within the police information system"[73], said criminalist Zeljko Cvrtila. In accordance with their authorities and needs, police officers are granted access to certain levels of classified information. This gives them "the access to the largest register of personal data in the Republic of Croatia"[74]. According to the provisions of the above listed regulation on information security, data from this database can be used for professional use only.

- **Monitoring data traffic and employee access to data systems**. However, "*it is simply difficult to control this. As far as I know, this process is very poorly monitored*", said criminalist Zeljko Cvrtila. "*Several thousand issues are checked every day. Although protected from hacking – this base is, he says, not difficult to hack*", he concluded[75]. As was previously mentioned, each policeman has been granted a certain level of access to the data via his/her password, but nobody checks with the employee afterwards why he or she has checked out specific information, said Cvrtila.
- **Training and awareness measures for civil servants on risks of IT corruption and safeguards**. Employees of the Ministry of the Interior are participating in various training and awareness raising projects on risks of IT corruption and safeguards. The examples of this safeguard measure against IT corruption are two projects aimed at strengthening the administrative capacity of the Ministry in the field of IT abuse: Strengthening of Administrative Capacities of the Ministry of the Interior in Fighting against Cyber Crime (a project with costs of 700,000 euros) and Regional Cooperation in Criminal Justice: Strengthening Capacities in the Fight against Cybercrime (the project costs amounted to 2.777,778 euros), as well as workshops on forensic network conducted by the Ministry of the Interior and the Croatian Academic and Research Network.
- **Code of Ethics**. According to the Code of Ethics "*each employee is responsible for the ethical usage of entrusted authority of access to personal data from the police databases*"[76]. Employees of the Ministry of the Interior are obliged to act in accordance with the Code of Ethics. Citizens can report unethical behaviour of civil servants to the ethics officers.
- **Auditing of the IT system**. According to the Regulation on the Internal Organisation of the Ministry of the Interior (Official

73 http://dnevnik.hr/vijesti/hrvatska/svaki-policijski-sluzbenik-ima-lozinku-za-razlicite-baze-podataka.html

74 Potrka, Nikola (2013) Normativna uređenost zaštite osobnih podataka u Republici Hrvatskoj. Policijska sigurnost 22(4): 509-521

75 http://dnevnik.hr/vijesti/hrvatska/svaki-policijski-sluzbenik-ima-lozinku-za-razlicite-baze-podataka.html

76 Potrka, Nikola (2013) Normativna uređenost zaštite osobnih podataka u Republici Hrvatskoj. Policijska sigurnost 22(4): 509-521

Gazette no. 70/12, 140/13), there are two internal organisations in charge of police information system audits. One is the Information Security Department, which performs monitoring of the organisation, the implementation and the efficiency of prescribed information security measures and standards, and the other is the Internal Audit Department, which performs audits of the information system.

- **Legislative safeguards**. Articles 266 to 273 of the Criminal Code (Official Gazette, no. 125/11, 144/12) defines criminal acts against computer systems, programmes and data: unauthorised and illegal access to computer systems or computer data (computer hacking); obstruction of computer system performance; damaging of computer data; unauthorised interception of computer data; computer forgery; computer fraud; and abuse of device. According to the criminal code, grave criminal acts against computer systems, programmes and data are considered those regarding computer systems and computer data owned by state and local authorities, as well as public companies. Finally, the Code includes criminal acts related to the child pornography via computer systems and cyber violence.

Once again, it is important to note that the safeguard measures listed here are only one part of the network of safeguard measures applied by the Ministry of the Interior. Information on other measures is not available to the public due to safety reasons.

The cases described above show that despite the legislative framework; prescribed procedures; the Code of Ethics; and various safeguard measures, the abuse of IT systems is still possible. The weakest link of the safeguard process is the individual with all his/her virtues and flaws. It is hard even to imagine a safeguard measure which could assure corruption-free behaviour.

Croatia case 11: Senior inspector misused confidential data to win the local elections

According to the relevant legislation on information security, the Ministry of Finance has prescribed various measures to protect against abuse of taxpayers data from their information systems. Due to safety policy, and the fact that documents that prescribe safeguard measures used to protect this system from abuse are for official use only, and as noted in the previous cases, it is impossible to list all of them. Those which have been disclosed, however, are listed above in case 10.

In a huge organisational system, such as the Ministry of Finance, employing over nine thousand people and with organisational units across the entire country, safety policy issues are the concern of several organisational units:

- The Information System Sector within the General Secretariat. This Sector, among others, perform tasks of organising, establishing and maintaining a unique information system for the Central Office of the Ministry; it takes care of efficient and accurate use of information-communication resources; organises and manages the process of development, analysis and return of safety copies of data; monitors the safety of communications and implements information system safeguards measures.
- The Information System Sector within the Tax Administration, among others, performs planning, development and use of the information system and educates users of the IT system.
- The Information System Sector within the Customs Administration, among others, performs planning, management, supervision and coordination of development, supply and work of business applications, IT services and technology; develops and implements policies of protection and grant rights to access the information system; determines measures and quality of service; assures making of safety copies of the information system; planning of the financial means for licenses, development and maintenance of the information system; writing strategy for IT system development; and educates users on the IT system of the Customs Department.
- The Service for Development and Support to the Operational-Informational System of the State Treasury, among other tasks, assures continuity and stability and needed level of protection of business procedures of the State Treasury; performs tasks of designing, optimisation, analysis, upgrading and standardisation of business procedures; as well as tasks of authorisation, safety and protection of data.
- The Department for Strategic Analysis and Information System of the Anti-Money Laundering Office, which, among other tasks, designs and develops information and sub-systems of this office; proposes bylaws and internal regulations in the field of system data and records protection in the office; maintains and supervises the system of data and records protection of the office.

Once again, it is important to note that the listed safeguards are only a part of the safeguard measures network applied by the Ministry of the Interior, but which are, due to safety reasons, not fully available to the public.

However, as in the previous cases, and despite the legislative framework, prescribed procedures, Code of Ethics and various safeguard measures, abuse of IT systems is still possible. The weakest link of the safeguard process is the individual with all his/her virtues and flaws. It is hard even to imagine a theoretical safeguard measure which could assure corruption-free behaviour.

Croatia case 12: You didn't spend a day of your life at work? No problem, you can still get a full pension!

Safeguard measures designed to prevent the abuse of the main register of persons receiving pension insurance and main register on users of pension insurance rights within HZMO are: 1) tracking of chronology of data change (by using user ID and date); 2) policy of data access approval according to the working position and usage of modern hardware and software protection measures. Apart from these main safeguard measures, there are also: 3) provisions of relevant personal data protection legislation; and 4) provisions of Ethical codex and internal audit. However, cases like this prove that all these safeguard measures can still be violated.

In the past two years, HZMO has become one of the first institutions to participate in the project of the integration of the Personal Identification Number (OIB) system, together with the Tax Administration of the Ministry of Finance, the Ministry of Public Administration, and the Ministry of Internal Affairs. *"The goal of introducing the OIB has been to create a unique personal identifier, which would be legally accepted by public legal bodies of the Republic of Croatia. As a result of creating the unique personal identifier in all official records, the prerequisites are made for computer data exchange among legal public bodies. Only by computer data exchange can public legal bodies exchange, economically and efficiently, the necessary data from official records for timely and consistent implementation of all administrative, tax and criminal proceedings"*[77]. Bearing that in mind, the OIB has been recognised as a strong instrument which will, among others, enable the systematic fight against corruption.

Before integration into the OIB exchange network, HZMO operated as an island within the state administration. It had its own database of users and was regularly paying them their pensions. As a data exchange among legal public bodies was not possible, after the death of a family member, other

77 http://www.mfin.hr/en/novosti/full-application-of-oib-personal-identification-number

family members were obliged to bring a death certificate to the regional HZMO service, which was the body that would have paid the pension to the now deceased. This procedure opened a window for possible frauds. If nobody took the death certificate to the regional HZMO service, the family could continue receiving the pension.

However, after September 2013, the integration of HZMO into the OIB network has closed this loophole. Since the precondition of computer data exchange among legal public bodies is possession of an OIB, the first step of HZMO was to ensure that all their users own an OIB. It was actually discovered that 125,867 pensioners out of 1.2 million did not have an OIB. The second step has been to deny the possibility of collecting pensions from the post office, and rather receiving a pension through their bank account only. If the HZMO users wanted to continue to receive their pensions, they were obliged to deliver HZMO their OIB.

The number of pensioners without OIB declined to 49,586 in April 2014 and consists of mainly foreign users. Through additional exchange of data with the Tax Administration of the Ministry of Finance; the Ministry of Public Administration; and the Ministry of Internal Affairs, on 8 April 2014, the payment of 9,593 pensions were stopped – 9,108 from abroad and 485 from Croatia. HZMO is still trying to find out the reasons why these pensioners did not deliver their OIB to them. *"Are these users in Croatia, are they still alive, does someone else take their pension and illegally gain money"*, said the minister of the labour and pension system, Mr. Mirando Mrsic and added: *"Are there any frauds, are these people in Croatia, where these pensions go, we want to clear these things. We are not talking about small amounts, but about more than 16.6 million euros and we want to pay this money to those who are entitled to receive them*"[78].

So far, the integration of HZMO into the OIB network showed that 26 families continued to receive pensions of deceased family members. Among them, there was a case where a postman regularly delivered pension payments to the family of a man who died 20 years ago! It is only in this one case that the state faced an actual loss of 65,000 euros. With the integration into the OIB system, cases such as those previously described are no longer possible as the data exchange among legal public bodies gathers and compares data and automatically notifies authorities on data inconsistency.

78 http://dnevnik.hr/vijesti/hrvatska/nema-oib-a-nema-mirovine-pod-povecalom-2-400-umirovljenika---309572.html

Kosovo

By Hasan Preteni and Driart Elshani

Introduction to examples of safeguards against abuse of IT

Public sector agencies are reliant on information technology (IT) systems for operational functions and many for their service delivery. It is important to ensure that the information maintained on these systems is accurate and complete. It is also critical that this information is easily accessible for legitimate purposes and at the same time protected from misuse. In Kosovo there exist only a few electronic registers and therefore cases of IT corruption are low since there is no space to make electronic data alteration. Instead, the cases that we chose demonstrate the lack of safeguards that protect the abuse of data and the IT systems in general.

All cases presented in chapter 1 of this study highlight the importance of having both, administrative (or legislative) and technical safeguards put in place and implemented by each corresponding institution. Moreover, what we learn from each of these cases is that the aforementioned safeguards have either not been put in place, or have not been respected. Even when the safeguards were created, they were incomplete or they lacked clear definition of procedures and roles to mitigate the risks of data, and general information technology systems, abuse. Kosovo must work harder to create and implement those safeguards, especially since Kosovo will implement many IT systems in the future and it has to mitigate the risks of data and information technology systems abuse. Kosovo has not yet taken any specific action to address those safeguards properly.

The safeguards presented herein would mitigate those risks and would prevent the misuse of information technology systems. In the future everything will be digital – i.e. paper usage would be only limited and hence new forms of abuse could arise that should be tackled by different methods. Those methods would rely on the safeguards presented herein.

Indeed, in this study we have proposed specific safeguards to protect data integrity and the integrity of IT systems in order to protect them from potential human abuse. We have put in place propositions for general guidelines and mechanisms for the electronic systems. Those safeguards and guidelines should be applied to each and every institution.

These standards and policies are designed to protect the IT systems and data against destruction, alteration or falsification. The safeguards that we propose in chapter 2 of this study could be adopted in the form of a policy for the entire spectrum of institutions in order to protect their IT systems from potential abuse.

- In terms of technical safeguards, besides the centralisation of some IT systems, all other technical safeguards were obviously missing. We have no information if additional technical safeguards have been put in place. However, we now know that in some agencies the general application and approval processes are being reviewed.
- In terms of organisational and procedural safeguards, no such safeguards were put in place. For example, the lack of clear definition of roles and responsibilities could have existed, or the "many eyes" principle could have been put in place. No additional safeguards of this nature have been put in place.
- In terms of monitoring employee access to data systems, organisations have learnt from this case that such measures should be put in place. Some of these measures, such as monitoring who accesses the data systems, are now available.
- In terms of training and awareness measures, no such measures existed and no such measures exist now. There are not even plans to have such measures.
- In terms of auditing, most organisations did not have any auditing when this case was discovered and we have no information if such measures exist now. Some organisations have since implemented an overall security audit and they are in the process of implementing the recommendations. However, these recommendations are only in terms of security such as defence from cyber-attacks and do not address the issues that arose in this case.
- In terms of legislative safeguards, there were none at the time of this case.

Moreover, what we mostly learn from this case is that data exchange between public bodies could be crucial in the battle to prevent this type of case from reoccurring. If the systems were interoperable between them then that would speed up the process; for instance, having an interoperable process for the verification of tax documents would make it very difficult to counterfeit these documents.

IT corruption measures in Kosovo

Safeguards should be put in place in order to properly detect, monitor, and take measures against cases of corruption. These safeguards should be broad and varied, including: technical safeguards, organisational and procedural safeguards, monitoring data traffic and employee access to data systems, training and awareness measures, internal or external auditing, and legislative safeguards.

Moreover, it would be advisable that a special institutional body be established in the country in order to protect and to prevent the data integrity and information technology systems integrity from any wrongdoing. It is notable to say that such a specialised body does not exist in Kosovo. In Kosovo there is a dedicated Agency for the Protection of Privacy and Data but this Agency only acts in the form of a watchdog for privacy. Its mandate is not sufficient and does not extend to the obligations of ensuring safeguards relating to information technology abuse.

Indeed, there is no institution whatsoever that deals with writing and enforcing safeguards and standards in this matter. Many cases of information technology abuse remain at large, often completely undetected. When we speak about safeguards it is worth mentioning that safeguards could be twofold: technical and administrative.

Administrative safeguards could be in the form of laws, normative acts and administrative regulations that sanction any wrongdoing related to the integrity of data and the integrity of information technology systems in general. Each and every institution would follow a clear regulations' infrastructure prescribed by law.

Technical safeguards could be in the form of Standard Operating Procedures (SOPs) that each institution should follow in order to protect them from data abuse and general information technology systems abuse. Every institution would follow up a checklist of SOPs that guarantees their maximum protection and resilience against such offences. The current administrative instructions have no technical SOPs whatsoever in them.

In terms of administrative safeguards, Kosovo has adopted a set of laws, strategies and administrative instructions (normative acts) that relate to the usage of information and communication technologies, but the legislative infrastructure so far does not address properly the issue of data integrity and abuse of information technology systems specifically or in general.

Cybercrime

Kosovo does not yet have a Computer Emergency Response Team (CERT) which could also be in charge of protecting IT systems. It is foreseen that CERT will be created in the near future. However, CERT would still be insufficient as by default CERT would deal only in a reactive form of protection against abuse, rather than providing proactive preventative measures.

Other measures

Other measures could also be used in fighting IT corruption. For example, data exchange between public bodies and the implementation of an overall interoperability framework could help prevent some of the cases, for instance case 2. Special measures in public procurement IT systems such as e-Procurement could also be deemed relevant. Kosovo is in the process of implementing an e-Procurement system. Also, measures such as open government data could also be desired. This would favour data exchange between public bodies. Kosovo is in the beginning phase of this process.

Laws, strategies, and administrative instructions regarding ICTs in Kosovo

Laws

The laws regarding Information and Communication Technologies (ICTs) that have been implemented from 2009 until now in Kosovo are shown in the following table:

Table 2 Implemented and modified laws from 2009 until 2014[79]

No	Naming of the law	In Action Plan?	Law no.	Date of Approval	The act and date of Promulgation
1	Law on the Protection of Personal Data	YES	**03/L-172**	29.04.2010	Decree no. DL-020-2010, Date 13.05.2010
2	Law on Prevention and Fight of the Cybercrime	YES	**03/L-166**	10.06.2010	Decree no. DL-028-2010, Date 02.07.2010
3	Law on Access to Public Documents	YES	**03/L-215**	07.10.2010	Decree no. DL-063-2010, Date 01.11.2010
4	Law on Information Society Services	YES	**04/L-094**	15.03.2012	Decree no. DL-010-2012, Date 02.04.2012
5	Law on Prevention of Conflict of Interest in Discharge of Public Functions	YES	**04/L-051**	31.08.2011	Decree no. DL-029-2011, Date 31.08.2011
6	Law on State Archives	YES	**04/L-088**	15.02.2012	Decree no. DL-007-2012, Date 01.03.2012
7	Law on Administrative Conflicts	YES	**03/L-202**	16.09.2010	Promulgated, in accordance with Article 80.5 Of the Constitution of Republic of Kosovo, Date 06. 10.2010
8	Law on Higher Education in the Republic Kosovo	YES	**04/L-037**	29.08.2011	Decree no. DL-036-2011, Date 31.08.2011

Strategies

The following strategies that have been adopted up until now:

- National Strategy for Information Society 2006-2012
- Electronic Governance Strategy 2009-2015
- E-learning Strategy for Kosovo 2010-2015 with the main objective

79 Data taken from the Assembly of Kosovo* - Department for Support Legal and Procedure (AK – DSLP) (2014)

to transform e-learning into an integral part of the overall national educational system
- Kosovo Education Strategic Plan 2011-2016 which contains eight priority programs including Capacity Building and Information and Communication Technology
- Strategy for Development of Pre-university Education 2007-2017

However none of these laws and strategies specifically addresses data integrity or information technology systems abuse.

Administrative instructions

Finally, the following administrative instructions (AI) have been adopted so far in the matter of IT:

1. A.I. no. 02/2010 for Information Security Management
2. A.I. no. 01/2010 on Security and Access to Database
3. A.I. no. 04/2010 for the Use of Electronic Official Post in the Institutions of the Kosovo
4. A.I. no. 01/2011 for The Management and Use of The Internet in the Institutions of Kosovo
5. A.I. no. 07/2008 to Strengthen Transparency and The Standardisation of the Internet Webpages in the Institutions of Kosovo
6. A.I. no. 03/2010 for Hardware and Software Usage
7. A.I. no. 02/2011 for the Government Portal for the Republic of Kosovo

Analysing the contents of these documents also reveals the following issues:

- The AI on Information Security has been formally released since 2010 but there was no socialisation program to ensure that all parties understood their responsibilities and obligations;
- The AI on Information Security describes technical policies and does not define the framework of a management system, including roles, responsibilities and authority;
- There is no clear relationship between the various Administrative Instructions or how they have been defined to meet certain requirements.

Moreover, these administrative instructions only partly address concerns such as access rights to databases and to the internet, instead remaining largely vague. Moreover its enforcement is rather cumbersome as no specific institution deals with compliance. Most of all, although the general opinion is that there exists a good legal infrastructure in Kosovo, one can see that many pieces are still missing and/or are largely incomplete. Kosovo must

still work harder to ensure that legislatively protected safeguards are well written, adopted, and are being complied with.

Technical Safeguards

Safeguards are so far mainly limited to simple password protection of individual users, encryption of data in some singular cases, and attempting to keep servers protected from physical interference. More sophisticated strategies and standards for technical safeguards in public IT is currently missing in Kosovo.

Macedonia

By Marjan Stoilkovski and Rozalinda Stojova

Institutional safeguards

In 2002, according to the articles of the Law on Prevention of Corruption, the State Commission for Prevention of Corruption (SCPC) was established as an independent body. In Article 1 of the Law, SCPC was given responsibility to apply measures and activities that prevent corruption in the performance of government, public power, office and policy; measures and activities to prevent conflicts of interest; and measures and activities to prevent corruption in performing activities of public interest by legal entities related to the exercise of public authority, as well as measures and activities to prevent corruption in companies.

Also in 2008, the Unit for the Fight Against Corruption was established. It is a dedicated organisational unit under the Organised Crime Department of the Ministry of the Interior. The responsibilities of the Unit for the Fight Against Corruption are to identify and investigate any types of corruption in the Republic of Macedonia.

Technical safeguards against unauthorised access and abuse of IT systems and monitoring data traffic and employee access to data systems

As part of the technical specification of information systems, regardless of whether they are outsourced or developed in-house, there are few practices applied and followed. Some practices are set up according to the respective law, but some of the most important are the ones established by practice rather than outlined by law. They aim to prevent usage of IT for corruption, and are considered among the most important requirements that must be met at the very beginning of the process of acceptance test. They are:

- Keeping logs for every access, addition, deletion or editing of data, and making the log files available upon request for the purposes of revision and audit. Besides keeping and archiving logs, no other operation is allowed.
- Providing different levels of identification and authorisation. The confidentiality of data level processed by the system influences the level and complexity of the identification and authorisation process. In all systems, different user roles are defined depending on their assigned privileges, starting with simple username and password for some, and for others, there are requirements for using digital certificates or even only allowing access to data from a particular working station in a strictly determined specific physical location.
- According to the Law for Electronic Management, in cases of outsourced development of systems storage and/or processing personal data, but not excluded in cases of in-house system development, one of the requirements is to establish development and testing environments, using testing data, while real live data is stored only in the production environment. This enables channelled and controlled access to the data, and only by officially assigned employees.
- Generating regular reports of user activity by different types of users and roles is also a requirement providing a regular way of monitoring users' activities. These reports are sent to super administrators and to top management.
- One of the best practices for a majority of local systems is sending mail and/or sms notifications to super administrator(s) and top management in cases where suspicious activities have been detected, or are in the process of being committed.
- To secure the system's internet connection when exchanging data between systems, and to prevent data communication interception, all institutions create/ establish VPN connections using encrypted data.

- In line with their work, front desk officers use working stations that have access only to the data their institution is in charge of, and they do not have internet access or access to other systems.
- The IT systems of the private and public sector are tested for vulnerability and possible system penetration. Although penetration testing is more widely used in the private financial sector, it is common that the public sector hires certified companies for penetration testing too, and use this method to prevent the IT systems from unauthorised access.

Organisational and procedural safeguards such as the 'many eyes principle'

- There is a trend of signing NDAs (Non-Disclosure Agreements) with the economic operators and implementers. These agreements are amended with statements for non-disclosure from both sides - contractor and implementer - for persons with system access.
- Physical access to systems at any point of time, whether is it during implementation or during maintenance, is possible only after obtaining clearance from the Ministry of Internal Affairs for each person involved.
- There is an adopted practice in the institutions of assigning two basic key roles to two different types of employees: technical administrators and content administrators. Technical administrators are responsible for the system on an application level, and besides managing the system and database, employees in this role also manage users and their permissions, but not the data stored/kept in the databases. The content administrator is responsible for managing data stored in the databases.

Training and awareness measures for civil servants on risks of IT corruption and safeguards

Victims of corruption might be an individual citizen, a business, or a group of entities, but in some cases the victim is society at large. The fight against corruption is one of the most important strategic goals adopted by the ministries and other institutions showing the commitment of the government of the Republic of Macedonia (i.e. see the Public Administration Reform Strategy and its Action Plan[80]). Furthermore, the public sector and

80 http://mioa.gov.mk/files/pdf/dokumenti/RevidiranAP_SRJA_mioagov.pdf

citizens play an active role in reforming society, proving the importance of their willingness and readiness to learn about ways of preventing corruption and the opportunities available for legal action. The following actions are therefore undertaken by the institutions and public sector (NGO): training of employees and citizens more frequently in the institutions that are more vulnerable to corruption; public awareness campaigns via different channels: printed flyers, billboards, short TV commercials.

Auditing of IT systems (internal or external audits; initiated by the state body, or by reports or complaints from citizens or the press)

Although auditing IT systems from internal and external audits is being done for a very small number of systems, it is one of the possible measures. It has been applied in very rare cases, such as when the system handles confidential data or data of importance for the state, and in cases where sufficient budget and time is allocated.

Legislative safeguards

In 2002 the **Law on Prevention of Corruption** was adopted enabling implementation of a legal framework in the fight against corruption. Last reviewed in 2010, this law:

"shall regulate the measures and activities for prevention of corruption in the exercise of power, public authorisations, official duty and politics, measures and activities for prevention of conflict of interests, measures and activities for prevention of corruption in undertaking activities of public interest by legal entities related to execution of public authorizations, as well as measures and activities for prevention of corruption in trade companies." (Article 1).

It introduced a system of integrity (integrity pact) and protection of "whistleblowers".

- The **Law for Electronic Management** describes standards that need to be met when developing information systems that communicate, and share data and documents, with information systems from other institutions for the purposes of administrative procedure[81]. The bylaw for recognising the unique environment and electronic communication between institutions for data and document exchange and with its subsequent guidelines for technical requirements, mode

81 http://mioa.gov.mk/files/pdf/dokumenti/zakoni/zeu/Zakon_za_elektronsko_upravuvanje_konsolidiran_tekst.pdf

of operation, communication client and recommendation for usage of interoperability system describes the:

- technical requirement of hardware and software infrastructure of the communicating clients;
- test environment;
- maintenance and development of web services;
- e-mail protocols;
- access to data, subject to exchange;
- data safety and integrity, and in subsequent guidelines many of the controls from the ISO 27000 standard series are introduced;
- data and document structure, subject of exchange; and
- planning of basic elements of architecture for communication with the interoperability system.

- **Law for Electronic Communication** provides protection of the rights of users, including end-users with disabilities and end-users with special social needs and ensures confidentiality of communications.
- **Law for Personal Data Protection**, last reviewed in 2012, is aligned with relevant EU directives and is applied to entirely or partly automated personal data processing. Among other topics, it describes ways of personal data processing and established required technical measures for protecting processing of personal data.
- **Law using data from public sector** adopted in 2014 is a reflection of the activities undertaken in the course of the Open Government Partnership Initiative. It is aligned with the Directive 2003/98/EC of the European Parliament and the European Council for public sector information re-use. "This law establishes the obligation of the authorities and institutions of the public sector for public disclosure of data generated by the exercise of their powers in accordance with law, in order to enable the use of such data by businesses or individuals to create new information, content, applications or services." One of the goals is to encourage "increased accountability and transparency of (the) public sector", which is one of the tools for prevention of corruption.
- **The Law for Financial Discipline**, adopted in 2013, regulates timely fulfilment of financial obligations arising from the implementation of business transactions between economic operators in the private sector, or between public sector entities and economic operators from the private sector, in order to prevent the failure of anticipated cash obligations in accordance with the terms of the law. Fines are determined for each contractor that does not comply with this obligation. Enforcement of controlled payment of cash obligations firmly supports anti-corruption activities.

- The last revisions of the **Law for Public Procurement** were made in 2014 with a few major changes. Prior to the procurements of goods and services that have a higher assessed value than what is defined monthly for small procurements, contractors are obliged to undertake market research. This means providing a certain number (depending on the assessed value) of requirement acceptances from different suppliers. If there are less than the prescribed number of suppliers capable of delivering the required good or service who are eligible to apply, a contractor must obtain written consent from the Council of Public Procurement, a body established with this revision of the Law.
- According to the national legislation for classified information, every IT System that holds or processes classified information, must be accredited by certified accreditors from the National Directorate for Classified Information. When developing IT systems for processing classified information, special directives are adopted for the technical characteristics of the hardware and the software that will be used in the IT system for classified information.
- Amongst other legal acts, the **Law for Classified Information** at national level is used like a safeguard against unauthorised access and abuse of IT systems.

Other measures

Safeguards in the procurement process and for financial discipline

In addition, the following requirements have been introduced that support prevention of corruption within public procurement procedures:

- technical specifications must not contain any brands, even associated with leading descriptions, and detailed requirements in specification should be met by more than one vendor; except in cases described by the Law where a pre-described process is respected;
- all public procurement of the state and public institutions must be executed via the system for public procurement.

Characteristic software application as a safeguard

The minister of the Ministry of Labour and Social Policy (MLSP) stated that the Ministry has conducted a series of activities and analysis in the field of social welfare rights. He added that with the implementation of new software for social welfare, cases of abuses and false disclosure of information by users had been detected. Deeper analysis revealed that such abuses could not have been conducted unless there was cooperation with several employees. Consequently, internal audits and monitoring of the work of social care centres has been initiated where in a few cases evidence of abusing the right to social welfare was found, and for all of them criminal charges were filed. It was proven that nine citizens from one city A, employed as officers in the public institution "Centre for Social Work" in city A, had abused and misused their official position and helped a specific number of citizens to obtain social welfare rights illegally.

In cases previously vulnerable to corruption, IT systems are now used to distribute CEMT licenses, social housing apartments, students' dormitory rooms and other services. One of the most important services is electronic distribution of court cases to judges, identified and presented as measure 11 in the Public Administration Reform Strategy and its Action Plan[82].

There is an electronic form for anonymous notification of corruption made or in progress, available on the portal of the Public Revenue Office (PRO). It is the most used form of this kind. Anonymity of the sender is guaranteed, by making his/her IP address invisible for the PRO users.

Open Government as a safeguard

Opening up public data and publishing them on institutional portals in one of the 5 star levels[83] formats, which - in a nutshell - is the Open Government Partnership Initiative. It is a new approach for anti-corruption activities and enables each subject to have an active role in preventing and determining corruption. For example, one of the types of data that is being published, if submitted, is data on financial and property/assets status of the high officials.

82 http://mioa.gov.mk/files/pdf/dokumenti/RevidiranAP_SRJA_mioagov.pdf

83 The five star Open Data plan as suggested by Tim Berners-Lee, inventor of the world wide web and initiator of open data, awards stars to how open and linkable a data format is. One star describes making data available on the web (whatever format) under an open license, but data does not have to be structured, can use proprietary formats, need not use URI to denote things, and need not be linkable to other data for providing context. One star is the lowest level of making data open.

As further evidence of the government's commitment, in 2014 the Law on Use of Data from the Public Sector was adopted. It establishes the obligation of the authorities and institutions from the public sector to publicly disclose data generated in the line of their responsibilities, in order to enable the use of such data by businesses or individuals to create new information, content, applications or services. This law also defines restriction for exclusive contracts by institutions.

Aligned with opening data, laws that treats issuance of professional licenses that end with the testing process, i.e. executors, forensic experts, evaluators, notaries and others, are being aligned according to the following principles: for each profession, there should be a pool of at least 500 predefined questions made publicly available on relevant portals. Testing is performed electronically only using electronic testing systems. A sample of questions on the real testing is randomly selected according to certain criteria and provides equal opportunities for all candidates. Moreover, testing should be video recorded or broadcasted via the internet and can be revoked if irregularities are noticed and proven.

This principle should be applied also in the employment process of administrative servants and in performing external testing of students, but in those cases with no video surveillance and by using different questions for each student.

Montenegro

By Dusan Drakic and Ivan Lazarevic

Introduction to examples of safeguards against abuse of IT

In order to reduce misuse of data we have to constantly monitor and develop certain aspects of ICT. However, in a narrow sense misuse of data at the national and sometimes local level is more likely a consequence of the moral status of society, and the unwillingness of the individual to subordinate to organised order and compliance. ICT enabled quality database registers, defined in accordance with international standards, provide the recognition, protection of domestic and foreign physical and judicial persons, as well as movable and immovable property within the national territory.

The cases selected draw attention to the need for a larger number of electronic registers, which will allow us to define the place of origin of data, as well as their online storage in a centralised database and to facilitate their use.

It is necessary to improve and standardise intra-government data exchange with a solid and reliable ICT infrastructure. It is important to modernise the public administration and expand user centric public services, increasing their availability and safe delivery through multiple channels.

The cases show that there is also the need to establish a framework of interoperability that will create the conditions for improving the quality of information management and exchange of information between government agencies, as well as allowing the automatic exchange and use of data stored in public registers and other information systems.

Safeguards in Montenegrin case examples

Montenegro case 1: Abuse of office and forgery of official documents

The case of an expired passport being falsified and used by a third person demonstrates the flaw or failure in the Ministry of the Interior information system for the issuance of passports, which should eliminate the risks of use and re-issuance of travel documents where the validity period has expired. The system did not tie the physical document (the passport) with a mirrored database record containing the exact same information, including the photo of the passport holder. Further, there were no electronic traces within the system identifying the officers who issued the forged passport.

The case demonstrates a lack of both technical and monitoring/auditing safeguards against abuse.

Travel documents are used internationally, and the case also demonstrates the need for electronic data exchange and verification between countries, such as is the case between the Schengen countries.

Montenegro case 2: Using IT data to inflict political damage

This is a case where the media was sent a false telephone listing which alleged that senior officials had been communicating with members of an organised crime unit.

The above example clearly shows that there is an issue of potential liability of the responsible persons in the operator company, primarily in relation to the confidentiality and the interception and abuse of electronic mail.

The most critical property of a company is data. Losing that data exposes a company to litigation and loss of reputation. Information stored in databases is important. Companies routinely store sensitive, private and proprietary information such as social security numbers, credit cards, payroll records, and personal information, to name a few. Companies must maintain and secure this information in a confidential manner otherwise they would expose themselves to loss of reputation and/or revenue.

The operator is obliged to provide required technical and organisational preconditions that allow the interception of communications, i.e. to enable the relevant state authorities to obtain retained data on traffic and location, but solely pursuant to a court's decision, if it is necessary for the conduct of criminal proceedings (according to the criminal procedure code), or for reasons of security of Montenegro (in particular according to legislation regulating intelligence services).

The case did not have a court epilogue and no objective or subjective responsibility was established. It is therefore not possible to establish exactly what safeguards were missing.

Montenegro case 3: Abuse of functions and entering incorrect data in public registries

This case concerned the illegal transfer of state-owned land in the municipal cadastre to a third person through unlawful edits of the cadastre. It involved production of a false electronic certificate that could later be used in a legal proceeding.

In Montenegro there is a combination of different electronic and physical land registries. Nevertheless, each year the number of registries grows. Some of the registries are digitised and data can in some instances be shared electronically. The same documents may have different origins and sometimes it is impossible to establish exactly who created them, and who has full access to documents. In this case it is a requirement that documentation is kept electronically, and access to registers is only allowed for authorised persons.

As a security principle, personnel should have exactly the access privilege level necessary to perform their job function or task. Granting a user privileges beyond their need is a common practice, which can lead to abuse of the excess privilege.

Monitoring users helps ensure:

- Data privacy, so that only authorised applications and users can view sensitive data.
- Data governance, so that critical database structures and values are not being changed outside of corporate change control procedures.

The case illustrates what happens when monitoring of employee access is insufficient. Further, edits of the municipal cadastre lacked organisational and procedural safeguards such as the 'many eyes principle'. No cross-checking was performed on the status of the land and ownership neither technically, nor by another employee in the municipal register or by an external audit.

Montenegro case 4: Illegal issuance of travel documents

In the Police Directory in Podgorica two requests for issuance of new passports were not verified by the clerk handling the cases. However, no electronic records in the information system regarding insurance of the passports were found by investigators, and all documentation on scanned requests for passports went missing from the filing room.

This example shows that there were no electronic records of scanned requests for issuance of passports in the information system, something which would eliminate the risks of using and issuing forged documents. It is also necessary to improve the electronic system security recording physical access to premises where files and official documents are kept.

Computers for database management and information system (servers) should be equipped with:

- a system for safe log-on and recording all accesses, so that the server access may be controlled and limited; and
- a mechanism for preventing unauthorised withdrawals and deposits of portable IT media, communication ports or connections for printing data.

Authentication is the verification of identity by a system or database based on the presentation of unique credentials to that system. Authentication contributes to the confidentiality of data and the accountability of actions performed on systems by verifying the unique identity of a user. Access to telecommunication, computer and application systems for data processing should only be allowed by entering the appropriate user name and corresponding password.

An increasing number of applications and e-Government Web services require / allow authentication and digital signature using a digital identity. In this case it is essential that all relevant documents are located in one place - an electronic register - and access to that register ought only to be available to authorised personnel who have the appropriate digital certificate.

Internal Certification Authority (CA) in the Ministry for Information Society and Telecommunications (GOV.ME) was established with the aim of using digital certificates to enable safe and reliable correspondence between state authorities. From the start, use of the digital certificate in public administration has actively been promoted and implemented by the Ministry for Information Society and Telecommunications (MIST). E-government services, both in MIST as well as in other institutions, are aimed at increasing the use of digital certificates, mostly for reasons of safe exchange of data and user identification.

IT corruption measures in Montenegro

In the last decade, awareness of corruption has increased in Montenegro and it has become an important priority in the political agenda of the country. Successive Montenegrin governments have committed themselves to fighting corruption and key steps have been taken to address the issue, in part because of commitments deriving from the European Union accession process and the subsequent need to adapt national legislation to *acquis communautaire*.

Information and communication technologies are an indispensable part of modern life. Integration of ICT in performing daily activities and tasks has become increasingly evident. In this regard threats to information and communication infrastructure that can threaten the availability, privacy and integrity thereof, may also affect the functioning of society as a whole. There are numerous ICT tools that can be used during various phases of combating corruption, including prevention, detection, analysis, and corrective action.

ICT is not a magic bullet when it comes to ensuring greater transparency and less corruption, or strengthening democracy.

- ICT can facilitate information sharing and social mobilisation and ultimately provide digital platforms where citizens can report incidents anonymously.
- ICT can facilitate the work of civil society organisations working towards greater transparency and against corruption by supporting a mix of methods of campaigning on transparency and educating citizens on what corruption is about and their civil rights.
- ICT can improve transparency in the public sector by increasing the coordination, dissemination and administrative capacity of the public sectors, as well as improving service delivery by employing user-friendly administrative systems.

ICT can, however, also intervene more directly. By automating processes, it is possible to significantly reduce opportunities for corruption by removing human agents at data collection and service delivery points – when people engage in e-banking there is no officer to bribe.

Here are some of the types of corruption ICT can – in principle – help combat:

- Automation: remove human agents and hence corruption opportunities from operations
- Transparency: remove opportunity for discretion
- Detection in operations: both details and aggregates from operations can be monitored to detect anomalies and unexpected performance
- Preventive detection: online social networks and individuals can be monitored to detect preparations for corrupt action
- Awareness raising: if the public is aware of government rules and procedures they are better able to resist arbitrary treatment
- Reporting: mobilising users/community to report cases will make it easier to take corrective action towards individuals and to reorganise systems to avoid "loopholes"
- Deterrence: publishing information about reported corruption as well as indicators (such as the imbalance between income and property) will deter civil servants from engaging in corruption.
- Promoting ethical attitudes: engaging the public by means of pursuing discussions in various online forums

It is very important to establish a data security procedure in order to avoid any problem in the field of IT abuse. It is necessary also to define some safeguards against the misuse of IT technology with the aim of committing an act of corruption.

The legislative framework

The legal documents that form the basis of the functioning of the basis for the further upgrade of the modern concept of information security in Montenegro:

- **Law on Information Security Measures** (Official Gazette of the Republic of Montenegro no. 14/10), provides the implementation of the measures and standards for information security, including the state of the confidentiality, integrity and availability of data. This law applies to state authorities, state government, local government authorities, legal entities and individuals who have access to or processing of data. This Act does not apply to information which provides information security in accordance with the regulations governing the confidentiality of data;
- **Law on Electronic Signatures** ("Official Gazette of the Republic of Montenegro", no. 55/03 and "Official Gazette of Montenegro", no. 41/10) regulates the use of electronic signatures in legal, administrative, judicial and other proceedings, as well as the rights, duties and responsibilities of legal and natural persons in relation to electronic certificates, unless regulations otherwise provided;
- **Law on Electronic Documents** regulates the manner of use of electronic documents in legal, administrative, judicial and other proceedings, as well as the rights, duties and responsibilities of companies, entrepreneurs, legal and physical entities, government bodies, state government, local government bodies and agencies and organisations exercising public authority in relation to electronic documents;
- **Classified Information Act** - the legal framework on security procedures for the exchange of classified information is in place and includes the Law on Classified Information and the Criminal Code as well as the Regulation on the manner and procedure assigning information classification and the Regulation on classified information evidence;
- The Law on Ratification of the **Convention on Cybercrime** - Montenegro adopted the Law on Ratification of the Convention on Cybercrime on 3rd March 2010, which entered into force on 1 July 2010. Criminal offences included under this Convention as cybercrime include a wide range of spreading viruses, unauthorised access to a computer network through piracy to pornography and intrusion into banking systems, abuse of credit cards, and all other criminal offences in which computers are used.

Other important documents that should be mentioned:

- Study with defined responsibilities of state authorities in fight against cybercrime including assessment of the state condition and readiness in the area of cyber security;
- Regulation on detailed conditions and manner of implementation of IT measures to protect classified information;
- Regulation on detailed conditions and manner of implementation of measures for the protection of classified information;
- Regulation on detailed conditions and manner of conducting industrial measures to protect classified information;
- Regulation on the performance and content of internal control over the implementation of measures for the protection of classified information.

Security controls

There must be security controls regarding IT corruption. "Information security controls are the technical, process and policy safeguards designed to protect sensitive data by mitigating the identified and assessed risks to its confidentiality, integrity, and availability"[84]. In the Ministry for Information Society and Telecommunication there is a directorate for information infrastructure which has three sectors: Project Analysis, Planning and Monitoring Unit; Infrastructure Services Unit; and Protection from Computer and Safety Incidents on Internet Unit – CIRT. Main CIRT goals are:

Prevention, treatment and elimination of consequences of computer security incidents on the Internet and other information systems security risks:

- Prevention is reflected in the proactive mode of action, which involves providing information and assessment of information security, vulnerability testing, collecting, recording and processing data on incidents, testing and implementation of new software and hardware systems for the protection of IT resources;
- Data processing and elimination of consequences consists of: determining the occurrence and severity of the incident, the cause of the incident, the mediation in communication between all parties involved in the incident, the reporting of other CERT / CIRT / CSIRT teams, preparation of reports and warnings to other users, eliminating vulnerabilities in the system, protecting systems against possible incidents, and forensic analysis.

84 http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Controls-and-Safeguards.pdf

User education in the field of information security includes:

- Setting publications, manuals, software tools and other useful information relating to safer use of information technology on the web portal (www.cirt.me);
- Organising courses and training on topics of IT security and the possible means of protection and prevention of computer-security incidents.

The Ministry for Information Society and Telecommunications have made several rulebooks:

- Rulebook on the measures and procedures for protection of certificates and data relating to the signers. This Rulebook regulates the organisational and technical measures for the protection of a certification system with regard to the protection of certificates and qualified certificates, data relating to signers, as well as the establishment and application of the system for protection of access to the certificate records;
- Rulebook on information security standards - establishes information security standards applied to implementation of information security measures stipulated by the regulation of the Government of Montenegro;
- Rulebook on Information Security Incident Management - CIRT shall develop and maintain a plan for responding to information security incidents reflected in defining the procedures relevant to incident management;
- Rulebook on the content and manner of keeping records and register of certification service providers. This document regulates the content and manner of keeping records of certification service providers, the manner of keeping the register of accredited certification service providers; as well as the minimum amount of insurance against the risk of liability for damages that may occur during the performance of certification services;
- Rulebook on electronic signature and advanced electronic signature protection measures. This Rulebook shall regulate electronic signature and advanced electronic signature protection measures, measures for verification of the signer's identity by the signer or the certification service provider in Montenegro, technical and technological procedures for advanced electronic signature creation and the requirements that advanced electronic signature creation devices are to fulfil;
- Rulebook of the mode and conditions for administrative access to the web portal of the Government of Montenegro;
- Rulebook of the use of computing and communication resources in the network of state organs;

- Certification Practice Statement – CPS.

Information security must also fulfill the conditions of confidentiality, integrity and availability of data. Information security focuses on data, regardless of its form: electronic, print or other forms of data.

Due to the constant growth of the number of services that state authorities and private sector entities provide to citizens, as well as to other legal entities, it is necessary to define a critical information infrastructure in Montenegro and develop protection procedures.

Key activities:

- Definition and protection of critical information infrastructure;
- Strengthening the resilience of information systems to incidents;
- Perform analysis of threats to IT infrastructure.

Data protection

In the Ministry for Information Society and Telecommunications, a Computer Emergency Response Team/Computer Security Incident Response Team - CERT/CSIRT (division for the protection against computer and security incidents on the Internet) has been established. Administrative agreement between the Ministry for Information Society and Telecommunications and the International Telecommunications Union has been signed in order to obtain specialised technical assistance for the needs of the establishment of the Computer Incident Response Team – CIRT (National team for processing and protection against computer incidents) which will operate in cooperation with CIRT's network established by the International Multilateral Partnership Against Cyber Threats (IMPACT).

Through the system of inspection surveillance, implementation of the Law on Information Safety and Regulation on Measures for Information Security has been provided which contributes to raising the level of data protection.

Primary constituency for CIRT.ME is defined as:

- All Government Institutions in Montenegro;
- Critical National Infrastructure in Montenegro.

Montenegrin CIRT was established in accordance with the Law on Information Security of Montenegro, within the Ministry for Information Society and Telecommunications (MIST). Formed as a separate organisational unit of the Ministry, it operates within the Department of IT infrastructure and will cover the area of the national CIRT. CIRT is engaged in the handling

of information security incidents if one party involved in an incident is in Montenegro (if it belongs to ".me" domain or if it is within Montenegrin IP address space).

CIRT Mission

- CIRT shall coordinate and assist government agencies in implementing proactive services to reduce the risks of computer security incidents as well as to respond to such incidents when they occur;
- CIRT.ME shall conduct awareness campaigns in order to educate the local population about the adverse effects of cyber threats and cybercrime.

Within the administration there must be a defined organisational hierarchy to be the most effective and long-term sustainable supply of the appropriate security information management.

Although there is a scarcity of reliable data, there is at least some evidence that ICT can be an effective tool to combat corruption. The potential of ICT can, however, only be realised when it is combined with real administrative reforms.

Technical Safeguards

These are the hardware and software controls to protect the LAN and WAN from unauthorised access or misuse, help detect abuse and security violations, and provide security for LAN applications. Technical safeguards include user identification and authentication, authorisation and access controls, integrity controls, audit trail mechanisms, confidentiality controls, and preventative hardware maintenance controls.

Passwords are a primary method used to control access to resources and are the most common authentication mechanism[85]. Ministry for Information Society and Telecommunications (MIST) is responsible for the administration of the government network. MIST provides Network Monitoring and Administration: the IT operations function is given the responsibility to ensure that communication links are maintained and provide users with the approval level of network access. There is a policy regarding passwords for the whole government network which determined the method for making the new password each month.

85 books.google.de/books?isbn=0080558712

Control Identification

The challenge for organisations is to determine the appropriate set of security controls, which if implemented and determined to be effective in their application, would comply with the stated security requirements by mitigating the impact or likelihood of each identified threat. For each security category, a variety of controls is necessary for a comprehensive and robust security framework.

The use of cryptography to protect user data from source to destination, which is called end-to-end encryption, is a powerful tool for providing network security.

The Ministry of Information Society and Telecommunications of Montenegro Government (MIST) managed infrastructure public keys (GOV.ME-PKI) for internal purposes of public administration in Montenegro. Within the MIST, a certification body with a single rooted Certification Authority was established, which certifies the civil servants of the Ministry of Information Society and staff of the Government of Montenegro. This system is implemented fully in accordance with relevant legislation, mainly the Law on Electronic Signature.

Currently there are plans to start using digital certificates for logging into each PC in government, but lack of funds is still an issue and obstacle for implementing such a measure.

Data Transmission

Sensitive data transmission, whether through FTP, system-to-system, or web form submission, should be performed only over a trusted path or medium with controls to provide confidentiality, integrity, and authenticity of content. All connections from an internal system or database to other systems outside the accreditation boundary should be authorised only through the use of system connection agreements, and the connection should be monitored and controlled on an on-going basis.

Strong cryptography and security protocols should be used to safeguard the data during transmission over open, public networks. The transfer of personal information from external parties to the organisation, usually through a web site, should be accomplished via secure servers using high-level encryption.

Currently, data transmission, or data exchange, is done through secure web services for purposes of specialised IT systems. Connection is provided through a secure network, and encrypted with digital certificates.

Specialised system for data exchange still remains a challenge for Montenegro. Currently we are preparing a project called "Enterprise service bus" which will enable government institutions to securely exchange data among themselves. But, lack of funds remains an issue in the implementation of this project.

Remote Access

The definition for remote access is any access to an organisational information resource by a user or system communicating through an external, non-organisation-controlled network or connection. The organisation may deem it necessary to provide remote access to data and systems for remote workers or to support operations at remote locations. In some cases, remote access is required periodically by vendors to make regular or emergency system support.

In the Government of Montenegro only the deputy ministers and ministers may have remote access to their computer on the GOV network.

In Montenegro, 88.3% of companies surveyed stated that they used computers in their operations during January 2012. According to survey results, 53.3% of the companies (who used computers in their operations) allowed their employees a remote access to e-mail systems, documents or company applications in January 2012.

As a result of the increased risks associated with access from outside the trusted perimeter, the organisation should implement policies and processes governing the conditions under which remote access is granted and terminated. Remote access should be granted based on authorised business needs, limited to the minimum privileges needed, and require management approval, with all approvals periodically reviewed and justified.

In Montenegro, only 27.9% of companies have the Rulebook that normatively regulates information security issues. There is also a very small percentage of companies that conduct assessment of employees knowledge about information security measures, only 26.9%.

Coordinated construction of organisational, institutional and management capacities, improving laws and regulations are important items of information security existence in Montenegro.

Serbia

By Nemanja Nenadic and Bojan Cvetkovic

Safeguards in Serbian case examples Serbia case 1: Sex at Belgrade Arena

According to the instructions of the Commissioner for Information of Public Importance and Personal Data Protection, the Ministry of the Interior (MoI) enforced short-term, medium-term and long-term measures to safeguard against IT-related corruption.

Short-term safeguards:

- Technical safeguards;
    - Any kind of technical access to any kind of IT system has to be logged for later audit and revision;
    - Key cards were introduced to limit access to the facilities storing data;
- Organisational and procedural safeguards;
    - Access to data has to be accompanied with written procedures, defining what data can be accessed, and access authorisation;
    - The number of employees with direct operational access to data has been reduced to the minimum needed for normal operations;
    - Use of electronic portable media within the facilities that store data is now strictly limited and accompanied with specific data access procedures or is completely prohibited (depending on the type of facility);
- Monitoring safeguards;
    - Separate video surveillance systems that directly monitor access to the IT subsystems for data storage were installed.

Medium-term safeguards against IT corruption included:

- Training and awareness safeguards;
    - Training of MoI employees related to risks of IT corruption;
- Auditing of IT systems;
    - MoI has made plans to introduce an internal IT audit as well as ISO 27001 standardisation in the near future.

Long-term safeguards against IT corruption included:

- Legislative safeguards;
    - Internal administrative regulations were updated to ensure that unauthorised access to data is now defined as not just a disciplinary, but also a criminal offence;
    - Internal administrative regulations were updated to include the specific stance within the MoI that the use of the data for any other purpose than the original one for which the data was collected is now defined as a criminal offence (not just disciplinary);
    - The internal administrative regulations concerning the procedures for use and application of specific types of electronic portable media (optical disc, memory stick, smart phone, digital camera, etc.) have been updated to limit or prohibit its use in MoI locations depending on the type of data that can be abused;
    - Article 42, paragraph 3 of the Constitution explicitly prohibits and punishes use of personal data beyond the purposes for which it was collected.

Serbia case 2: When an IT contractor "takes root"

The real-life case exposed MoJ dependency on its IT contractors and revealed a number of different types of IT contractor related risks. Safeguards that had been initiated included short-term, medium-term and long-term measures to significantly reduce IT contractor related risks.

Short-term safeguards against IT corruption included:

- Technical safeguards;
    - Any kind of technical access to any kind of IT system has to be logged;
    - Physical security systems were introduced as a measure to limit and control the access to the MoJ data centre that centrally stores all data;
- Organisational and procedural safeguards;
    - Access to data has to be accompanied with the official request and approval (permission) from the specific court (or prosecutor office) for accessing specific case(s);
    - Nobody, not even the highest level of MoJ employees, have access to the data without prior approval (permission) from the court (or prosecutor office);

        - Each court (or prosecutor office) can access only their own data - access to data belonging to other entities is prohibited;
        - IT contractor employees cannot access the central data centre nor data itself without being accompanied by a minimum of two ministerial employees;
        - The number of employees with direct operational access to data has been reduced to the minimum needed for normal operations;
        - Any kind of IT systems upgrade or update has to be done within the central data centre - no remote access is allowed for anybody;
        - Use of electronic portable media within the facilities that store data is completely prohibited;
    - Monitoring safeguards;
        - A separate video surveillance system that directly monitors access to the central data centre where all data is stored was installed.

Medium-term safeguards against IT corruption included:

- Training and awareness safeguards;
    - Training of MoJ employees related to the risks of IT corruption;
- Auditing of IT systems;
    - MoJ has already introduced an external IT audit;
    - MoJ has plans to introduce ISO 27001 and ISO 20000 standardisation in the near future.

Long-term safeguards against IT corruption included:

- Legislative safeguards;
    - Internal administrative regulations were updated to include a prohibition on unauthorised access to data within the MoJ;
    - Internal administrative regulations were updated to include data access being in line with the "separation of powers" between ministry, courts, prosecutor offices and prisons;
    - Internal administrative regulations concerning the procedures for use and application of specific types of electronic portable media (optical disc, memory stick, smart phone, digital camera, etc.) were updated so as to prohibit its use in the central MoJ data centre location;
    - Public Procurement Law ("Official Gazette of Republic of Serbia", no. 124/12).

Serbia case 3: A General Manager spying on employees

It is not known what measures have been undertaken to close the gap in the Privatisation Agency regarding prevention of the abuse of IT since the case presented has clearly indicated the human factor weakness in the Privatisation Agency that was the key and focal point of abuse of IT.

Serbia case 4: "Road mafia"

As explained in the "Road mafia" verdict, safeguards from IT corruption did not function for years. Members of the gang were informed in a timely manner about controls, so they had enough time to hide evidence of the crime. Controls were usually conducted after 6 PM, when the gang did not operate. Furthermore, despite the fact that the file EMU-87 was fake and different from the original one, the truth remained unknown for years. Since the electronic system for payments and registration of vehicles functioned "normally", no control identified this interruption. The employee from the company that maintained the "Serbia Roads" electronic system had administrative powers, and it seems that no one from the "Serbia Roads" oversaw their work.

The system for registration of individual toll collectors with their unique ID did not function in practice. ID numbers were visible to colleagues and shift managers made frequent replacements of employees.

Short-term safeguards against IT corruption included:

- Technical safeguards
    - Complementary but separate sensor based IT system was installed in order to track the types and quantity of the vehicles passing the tolls (now the statistics from the original system must match with the new sensor based system)
    - Physical security systems have been introduced as a measure to limit and control the access to the facilities that store user data

We have no information if and what kind of organisational, procedural and monitoring safeguards were taken.

We have no information if and what kind of medium-term safeguards against IT corruption were taken.

Long-term safeguards against IT corruption included the introduction of a new type of toll payment service called "ENP" (in English, "Electronic Toll Payment") that is completely based on electronic payment via NFC cards in order to avoid any direct cash transfer between the parties at the toll.

Proactive publishing of information – tool to prevent IT corruption

Serbian Law on Free Access to Information ("Official Gazette of the Republic of Serbia", no. 120/04, 54/07, 104/09 and 36/10) provides for mandatory publishing of an "Information booklet" for all public institutions (funded from the Budget), a document whose content is defined through the 'Instruction of the Commissioner' (last issued in 2010)[86]. The information booklet has to be published online and updated at least monthly. This publication is meant to provide a lot of useful information to hold government bodies accountable, such as public procurement, budget, donation, and state aid data. Other information is about the structure of government bodies or the services they provide to the citizens. However, for this analysis, the most interesting parts are the provisions of Articles 37, 38 and 39.

Article 37 deals with "storing of information carriers". Information carriers are media where data is stored; such as papers, hard discs, databases, videotapes, etc. A public authority must identify various types of such media used to store information, by type, quantity (exact or estimated), as well as the type of data that they are storing. Furthermore, authorities must identify where "information carriers" are stored (organisational units or specific areas within the authority, such as archives, libraries, and electronic databases) and the storage places inside these premises (e.g. metal cabinets, shelves with folders, common server or individual computer equipment). Public authorities are required to describe briefly how information carriers are kept and maintained in practice (whether the secure recording of data to another carrier is carried out, whether the computers are protected from viruses, if anyone other than employees has access to the information carrier, whether there is periodic review of compliance with the requirements for storing information carriers, etc.) and to indicate whether the storage conditions comply with the regulations or the need to preserve them, if there are no such regulations.

Articles 38 and 39 forces public authorities to mandatory publish information about the types of information in its possession and the types of data for

86 http://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/uputstvo-informator/uputstvoen.doc

which access will be granted. The types of information may be, for example (as listed in Instructions), the following:

- The collection of regulations
- Issued opinions
- Minutes of meetings
- Decisions
- Appeals
- Concluded contracts
- Sound and video clips from events organised by the state authority
- Citizens' letters
- Various types of communication with the public
- Documents on payments, employees, public procurement
- Drafts of the documents in preparation
- Official records
- Clients' requests and applications, etc.

Information about data availability should be given in such a way that a comparison with the list of possessed types of information is made possible. If the information is accurate and comprehensive, the public could hold authorities accountable and it may prevent, among other things, situations where civil servants claim that certain information is not possessed by the authority or that information is lost, etc. In reality, most of the authorities are not complying and do not provide in details neither information on data carriers nor information on data types. This situation is expected to change very soon with the expected amendments to the Law on Free Access to Information that will make oversight and sanctioning procedures more efficient.

Criminal offences in place, implementation unknown

The Criminal Code of the Republic of Serbia (Official Gazette of RS, no. 85/2005, 88/2005, 107/2005) with added amendments from 31 August and 29 December 2009, and 24 December 2012, provides sanctions in chapter XXVII for criminal offences against the security of computer data.

The first criminal offence within this group is *"Damaging computer data and programs"* (Article 298). A person may be punished by fine or imprisonment of up to one year if he/she *"without authorisation deletes, alters, damages, conceals or otherwise makes unusable computer data or program"*. In cases where damages are greater, it can mean imprisonment of up to five years. Equipment and devices used in the perpetration of the offence shall be seized.

"Computer sabotage" (Article 299) envisages punishment of up to five years for:

"the one who enters, destroys, deletes, alters, damages, conceals or otherwise makes unusable a computer or program or damages or destroys a computer or other equipment for electronic processing and transfer of data, with the intent to prevent or considerably disrupt electronic processing and transfer of data of importance for government authorities, enterprises or other entities".

"Creating and Introducing of computer viruses" (Article 300) defines a punishment of up to six months for *"the one who makes a computer virus with the intent to introduce it into another's computer or computer network*". If the offender *"introduces a computer virus into another's computer or computer network thereby causing damage"* the punishment would be up to two years imprisonment. Equipment and devices used for committing the offence shall be seized.

"Computer fraud" (Article 301) is defined in following way:

"Whoever enters incorrect data, fails to enter correct data or otherwise conceals or falsely represents data and thereby affects the results of electronic processing and transfer of data with the intent to acquire for himself or another unlawful material gain and thus causes material damage to another person, shall be punished by fine or imprisonment of up to three years."

For more valuable proceedings of crime or damage, the punishment may be up to ten years.

"Unauthorised access to computer" and "Computer network or electronic data processing" (Article 302) could be punished with up to three years, depending on the damage.

Preventing or restricting access to a public computer network (Article 303) is punishable with up to three years.

"*Unauthorised use of computer or computer network*" (Article 304) defines that:

"Whoever uses computer services or computer network with the intent to acquire unlawful material gain for himself or another, shall be punished by fine or imprisonment up to three months. Prosecution for this offence specified shall be instigated by private action."

The latest amendment from this group is *"Manufacture, procurement, and provision to others as means of committing criminal offences against the security of computer data"* (Article 304a):

"Whoever possesses, manufactures, procures, sells, or gives to others for their use computers, computer systems, computer data or software intended for committing one of the criminal offences referred to in Articles 298 through 303 herein shall be punished with imprisonment of six months to three years. Items referred to in paragraph 1 hereof shall be seized."

Serbia also has a wide range of criminal offences that may be used to punish corruption (abuse of power, bribe taking, bribe giving, trading in influence, etc.), offences that are almost entirely compliant with the relevant international standards. One could draw the wrong conclusion that the criminal law system to fight IT corruption is effective. However, this is hardly the truth. The overall number of cases where corruption (IT or other) is fully investigated and finalised is still rather low and, particularly for cases involving high-ranking public officials or high amounts of money, is still extremely rare. The situation is not much better when it comes to the investigation of IT related crime in general. Serbia has had a special prosecutorial unit to fight cybercrime for years. This unit, in operation since 2006, still has a web page "under construction"; with the most recent statistics already three years old[87].

Lessons learnt – Safeguarding against using corruption using ICTs in the Western Balkans public sector

By Louise Thomasen

The individual safeguards listed in the introduction and described throughout this chapter, highlights how one safeguard can never stand alone. Safeguarding against ICT corruption requires that all described safeguards be in place, as they support and supplement each other. eGovernment is never a purely technical issue. eGovernment is not only about technology – it is about public administration too; and how we do things, how we cooperate within government, public administration, the community, economy and society as a whole. eGovernment must never be seen as isolated and independent from the rest of society.

Fighting corruption is becoming a priority for the Western Balkan countries in the ReSPA network. Several national authors note how the case examples

87 http://www.beograd.vtk.jt.rs/

highlight the need for increased awareness of the specific issues related to corruption and eGovernment, however the focus and measures differ. In Albania, the new Albanian government has updated its agenda of fighting corruption, and has recently introduced a new procedure on information system acceptances. In Bosnia and Herzegovina, national and domestic reports assert that corruption is amongst the biggest problems in society, and the European Commission 2013 progress report for the country states the lack of strategy and institutions to fight cybercrime and threats. In Kosovo the national authors observe that there are no institutions whatsoever that deal with writing and enforcing ICT safeguards and standards, and that many cases of ICT abuse go completely undetected, while the Serbian national authors remark that the overall number of cases where corruption (with or without ICTs) is fully investigated is rather low, especially cases involving high-ranking officials or high amounts of money. Even though Serbia has had a special prosecutorial unit since 2006 to fight cybercrime, not much information from that unit is available.

The Montenegrin authors observe that awareness of corruption has increased and has become an important priority on the political agenda in the country, and not just for the current government. In the Montenegrin Ministry for Information Society and Telecommunication there is now a directorate for information infrastructure with three sectors: Project Analysis, Planning and Monitoring Unit; Infrastructure Services Unit and Protection; and the CIRT (Computer Incident Response Team). The Montenegrin authors also highlight several studies and regulations on fighting cyber crime and protecting information. In Montenegro, fighting corruption is also one of the most important strategic goals for the government. In addition, the Montenegrins also organise public awareness campaigns, training of employees and citizens on ways to prevent corruption, inform on opportunities available for legal action, as well as offer government commitment in the Public Administration Reform Strategy and Action Plan. In Croatia there is a body of legislation for information security, as well as specific central state authorities in charge responsible for protecting "integrity and availability of the information system in the process of planning, designing, making, using and cease of work of the information system".

We cannot make a direct comparison between the countries to determine how far the countries are in combating ICT corruption, as we have no statistical data to support us. However, from the contributions from national authors we can tentatively discern between the national efforts, and it seems that Croatia, Macedonia, and Montenegro are more diligent in safeguarding public sector ICT use from abuse and corruption than the other countries in this study.

Technical safeguards - access to data

ICT in the public sector can enable increased transparency in who accesses and uses public sector data. But it can also enable much wider abuse than is possible without ICT, such as falsifying data, illegal obtaining of data and destruction of data.

Again let us stress that our case examples do not constitute a representative sample, but what is evident from Table 3 is that we see more cases of falsifying data rather than illegal obtaining of data, and the fewest cases concern actual destruction of data.

Table 3 Case examples of abuse made possible by access to data

Falsifying data	Illegal obtaining of data	Destroying data
Bosnia and Herzegovina case 3: Misuse of CIPS project's electronic system	Croatia case 1: Call doctor for votes	Bosnia and Herzegovina case 2: Another controversial employment in Supreme Audit Institution of the Republic of Srpska
Croatia case 8: Every year 2 million euros disappears from the tollbooths	Croatia case 11: Senior inspector misused confidential data to win the local elections!	Croatia case 6: Policeman deleting traffic offences and disclosing confidential data: they accepted even roasted lamb and 20 litres of wine as a bribe!
Croatia case 12: You didn't spend a day of your life at work? No problem, you can still get a full pension!	Croatia case 2: Confidential Croatian radio-television database on the black market	Croatia case 8: Every year 2 million euros disappear from the tollbooths
Kosovo case 1: Destruction of evidence	Croatia case 3: In search for veterans	Kosovo case 1: Destruction of evidence
Kosovo case 2: Gaining the war invalid status	Croatia case 4: With a little help from civil servants 68 Croatian passports were sold to criminals	
Kosovo case 4: Falsifying of the tax document	Croatia case 6: Policeman deleting traffic offences and disclosing confidential data: they accepted even roasted lamb and 20 litres of wine as a bribe!	
Macedonia case 1: Abuse the IT system on pay tolls	Croatia case 7: Accidentally caught for disclosure of confidential data on cars and their owners!	

Macedonia case 3: Abuse of IT system and illegal disclosure of personal data	Montenegro case 2: Using IT to inflict political damage	
Macedonia case 4: Misuse of registering working hours system	Macedonia case 3: Abuse of IT system and illegal disclosure of personal data	
Montenegro case 1: Abuse of office and forgery of official documents	Serbia case 1: Sex at Belgrade Arena	
Montenegro case 2: Using IT to inflict political damage		
Montenegro case 3: Abuse of functions and entering incorrect data in public registries		
Montenegro case 4: Illegal issuance of travel documents		
Serbia case 4: Road mafia		

Safeguarding access to data therefore becomes paramount, and includes not just access control, but also using appropriate levels of access.

Access control - passwords and user ID management

Control of and limits to system access are done through assigning personnel user identification and passwords. Most systems sharing data, or serving more than one user, have some kind of access control, user ID and password scheme. In standalone systems, data and computer programs should be secured by access control to the computer itself. It may seem self evident that access should be limited to authorised users, but this is not always the case.

In the Serbian case 4 (Road mafia) example, the system for registration of individual toll collectors with their unique ID did not function in practice. ID numbers were visible to colleagues and shift managers made frequent replacements of employees. In the Macedonian case 5 (Abuse of administrator's rights - bank guarantees/import quotas), an employee with administrator rights discovered that he kept access privileges after his transferral from one administrative centre to another. He then created a fake user account and used it to temporarily alter bank guarantee data, and in coalition with a local

company commit fraud at the border. The super administrator did not perform regular checks and revisions of the privileges of re-allocated administrators, and the administrator was thus able to commit offences using a newly generated user account. In other cases, misuse or stealing of passwords such as in Kosovo case 3 (Misuse of password), Bosnia and Herzegovina case 1 (The most famous Bosnian hacker amongst the prosecutors), and Albania case 2 (Corruption in the Electronic Public Procurement System), opens opportunities for corruption. Although the e-procurement system used in Albania seemed to observe all necessary precautions, the email system used for supporting the e-procurement system undermined all good intentions, as it was revealed when the procurement evaluation was made by a third person after a change of password. In reality, all the users knew each other's passwords. Although this practice was implemented with the good intentions of solving working issues, it reduced system security overall.

Passwords and user ID should always be personal and confidential. What might start as a convenient way to make everyday working life manageable, such as lending passwords to colleagues or subordinates for immediate task resolution, or resetting passwords to a default value known by others and thus not secret any longer, can be abused as demonstrated in the examples above. If it is necessary to delegate access to systems and data to a colleague, systems should allow for it, but in such a way that: 1) the employee will use his/her own personal ID when logging on to the system; 2) log files are kept of access to system and data; and 3) only limited and targeted access is granted and it can expire.

Appropriate access level to data and systems

Several cases explicitly highlight what can happen when access levels to data are inappropriate, i.e. grant wider access to systems and data than what is strictly necessary for the employees' immediate tasks.

In the Macedonian case 5 (Abuse of administrator's rights (bank guarantees/ import quotas) and Montenegro case 3 (Abuse of functions and entering incorrect data in public registries), the employees had much wider access to alter or insert data than what was strictly necessary for them to do their job. In both cases they abused their functions and made it possible to present data/documents that looked legal to outside parties.

Physical access to data and documents

Physical access to facilities that store data or physical copies of data for verification, legitimisation etc. should be restricted to authorised personnel, whose access is both logged and monitored.

In the Croatian case 2 (Confidential Croatian radio-television database on the black market) a copy of the Croatian radio-television licence fee database (the HRT Register) was sold on the black market. Physical access to the server room storing the HRT Register is granted exclusively to authorised persons, but access to the database is also available through a local network and the internet using protected data tunnels. Regardless of whether the database was copied directly from the server in the server room or remotely, the Croatian authors remark that standards to limit physical access have not been applied.

In the Montenegro case 4 (Illegal issuance of travel documents) the authors write that it is necessary to introduce document scanning or establish electronic databases of all documents submitted and issued in hard copy with mandatory double back up option, in order to ensure the security of data in the event of their intentional or accidental destruction. Also, it is necessary to improve the electronic system security recording physical access to premises where files and official documents are kept. Even more complicated is the Montenegrin case 3 (Abuse of functions and entering incorrect data in public registries), where there is a combination of different electronic and physical land registries. The same documents may have different origins and sometimes it is impossible to establish exactly who created the documents and who has full access to them. In this case it is a requirement that documentation is kept electronically, and access to both physical and electronic registries is only allowed for authorised persons.

In the Serbian case 1 (Sex at the Belgrade Arena) key cards have now been introduced to limit access to the facilities storing data. Use of electronic portable media within the facilities that store data is now strictly limited, and is now accompanied with specific data access procedures or has been completely prohibited (depending on the type of facility).

In Montenegro physical access to systems, whether during implementation or maintenance, now requires obtaining clearance from the Ministry of Internal Affairs for each person involved.

Security procedures and standards

The Bosnian, Macedonian, Montenegrin, and Serbian authors refer to implementation of the ISO 27001 standard on Information Security Management and the ISO 9001 Quality Management standard, as concrete safeguards implemented as security procedures to ensure data safety and integrity. In Bosnia and Herzegovina the judiciary has improved security procedures such as those mentioned in the ISO 27001 security

procedures at all levels and implemented standard ISO / IEC 27001:2005. In Serbia, the Ministry of the Interior and Ministry of Justice both plan to introduce the ISO 27001 in the near future. In Montenegro, a rulebook on information security standards establishes information security standards applied to implementation of information security measures stipulated by the regulation of the Government of Montenegro. In Macedonia, the Law for Electronic Management describes standards that must be met when developing ICT systems that communicate, share data and documents in the public administration. In the bylaw, subsequent guidelines on implementing many of the controls from the ISO 27000 series are introduced.

Backup and log files

Log files ensure that a system can be audited later to establish exactly who did what and when. The same holds true for backup files, as backups are a recording of what data looked like at a specific point in time.

In Kosovo case 1 (Destruction of Evidence) the entire material investigators expected to find on the Ministry of Public Administration's servers, and which would prove the suspicions of the Anti-corruption Agency concerning irregularities and violations of the law, were deleted from the government servers. What is even more aggravating in this case, is that for all public administrations in Kosovo, the servers for storing the data of all government institutions are located within this Ministry. That data was deleted from what one should assume to be the best-protected data environment in Kosovo.

In the Macedonia case 4 (Misuse of registering working hours system) investigation into the log files was paramount to revealing the abuse. The Macedonian authors remark that some practices are now set up according to the respective law, but some practices are established without having a formal basis in laws or by-laws. Amongst these practices are keeping logs for every access, addition, deletion or editing of data, and making the log files available upon request for the purposes of revision and audit. Besides keeping and archiving logs, no other operation is allowed.

Finally there is the case of the IDDEEA (Agency for Identification Documents, Registers, and Data Exchange) in Bosnia and Herzegovina responsible for establishing an electronic data exchange between police authorities and prosecutors, which started an activity leading to the new generation of data exchange in BIH. Amongst the requirements is data backup on remote location with good password protection combined with physical security.

Interoperability between public bodies' ICT systems and the establishment of base registries

Interoperability is the term used to describe the ability of diverse systems and organisations to work together (inter-operate). For systems to be interoperable, they need to exchange data. Barriers to data exchange typically include technical, semantic, organisational, and legal barriers, but one additional component could be added – trust. To expose one organisation's data to another, there needs to be some degree of trust between the parties in the exchange; otherwise experience tells us that cooperation will quickly cease to exist. Guaranteeing the integrity and safeguarding of data against abuse is of major importance for interoperability, and crucial for realising eGovernment potential for administrative burden reduction through the integration of eGovernment tools: the smart use of the information that citizens and businesses have to provide to public authorities for the completion of administrative procedures; making electronic procedures the dominant channel for delivering eGovernment services; and the principle of the 'once only' registration of relevant data. The latter ensures that citizens and businesses supply certain standard information only once, because public administration offices take action to internally share this data, so that no additional burden falls on citizens and businesses.

Of special importance is safeguarding the integrity of a country's base registries. Base registries are the basic building blocks of modern eGovernment within a country and increasingly between countries. They consist of the main databases containing up-to-date categories of everything the government and the public sector need to become an efficient administration offering good services (both electronic and non-electronic) to citizens and businesses, as well as developing and implementing effective policies. Base registries are the embodiment of the 'once only' principle. The most typical registries contain details of all citizens (birth, marriage, deaths, addresses, citizen identification numbers, passports/ID cards etc.) and of all companies (size, year of establishment, number of employees, sector of activity, tax liable and paid, often also linked to registries showing annual turnover, profit, etc.). Land and building registries are also common, as are registries on vehicles, transport networks, waterways, etc. Base registries can eliminate duplication efforts by public authorities, and decrease the likelihood of errors. Building base registries, and the interoperability system needed for them to be shared by relevant ministries and agencies, is thus a main foundation of eGovernment.

However, if public ICT systems are compromised or vulnerable to abuse, the consequences can be far reaching and have severe economic, societal, and legal implications for all, be they public administrations, citizens, businesses, etc.

In the Croatian case 12 (You didn't spend a day of your life at work? No problem, you can still get a full pension!) data integration and basic registry consolidation between authorities, using a national personal identification number (the Person Identification Number "OIB" exchange network) achieves the 'many eyes principle' safeguard, and as such solved the problems described in the case when the Croatian Pensions Insurance Institute (HZMO) was integrated into the OIB exchange network and audit of pensioner data took place.

The cases in chapter 1 include both examples of what constitutes base registries such as the Bosnia and Herzegovina case 3 (Misuse of CIPS project's electronic system) and the Montenegro case 3 (Abuse of functions and entering incorrect data in public registries).

In the Bosnian case it is noted that from the start of the Citizen Identification Protection System (CIPS) project in 2002 there were a number of complaints - particularly when issuing personal identity cards and passports throughout the country. That such a central register is compromised is very critical, and the Bosnian authors observes that even through the Agency for Identification Documents, Registers and Data Exchange (IDDEEA) now responsible for the CIPS have implemented a wide range of safeguards and complies with standards of a very high level of ICT safety and security, there are still problems in relation to data exchange with other authorities, a lack of institutional arrangements to coordinate eGovernment activities, and failure to implement IDDEEA guidelines throughout the public administration. This cannot only compromise the CIPS system, but also the willingness of public authorities to make their systems interoperable.

The Montenegrin case 3 concerns the municipal cadastre where unlawful edits of the cadastre enabled the illegal transfer of state-owned land in the municipal cadastre to a third person. The case involved production of a false electronic certificate that could later be used in a legal proceeding. There is no mentioning of lessons learnt and additional safeguards implemented in this case. But the case illustrates what happens when monitoring employee access is insufficient and how it can compromise the entire register.

Macedonian case 5 (Abuse of administrator's rights (bank guarantees/import quotas)) illustrates what happens when one public authority – the border

officials – is dependent on information and data from another authority as guarantee of third party information (bank guarantee), and where the value limited by the actual bank guarantee is being entered by the administrative officers instead of being acquired directly from the banks information systems. The authors do not mention any consequences on the collaboration between the public authorities involved, but caution and requirement for data integrity could be expected.

Monitoring and auditing

Backups and log files are 'technical' enablers of the monitoring and auditing safeguards, but there are a few other issues relevant when accounting for the need to monitor and audit ICT systems.

Between systems and processes – the weakest link

Several cases from chapter 1 illustrate how the organisation must safeguard all its processes as well as individual steps from both electronic and physical abuse. Even 'perfect' ICT systems are only as safe, and data is only as reliable, as their input. If false data is inserted into ICT systems, the integrity of the whole system is compromised. Monitoring and auditing must extend to all business processes and systems regardless of whether they are physical or electronic.

In the Albanian case 4 (Embezzlement and forgery in bookkeeping) an employee responsible for bookkeeping embezzled money by forging the payroll through receiving approval in writing (physical copy) and then later altering the electronic data for the payroll as well as the data sent to the bank. As there was no auditing on the concordance between the physical copy and electronic records, the weak link was between these two "procedures". The Albanian authors also mention the lack of checks by the financial system which was unable to simultaneously process individual details of the payroll against the total amount. Further, there was a missing cross-check between different signed documents for the payroll between financial authorities.

In the Kosovo case 2 (Gaining the War Invalid status) the abuse was committed during scanning, where the medical report was falsified. The perpetrator F.M. had supplied a document with which he presented that during the war in Kosovo he had medical problems. The document is not from the war period, but was drafted 5 years later. It contained the dates as if it had been drafted during the war.

The example of an expired passport being falsified and used by a third person in the Montenegro case 1 (Abuse of office and forgery of official documents) demonstrates the flaw or failure in the Ministry of the Interior (MoI) information system for the issuance of passports, which should eliminate the risks of use and re-issuance of travel documents where the validity period has expired. The system did not tie the physical document (the passport) with a mirrored database record containing the exact same information, including the photo of the passport holder. Further, there were no electronic traces within the system identifying the officers who issued the forged passport. The system vulnerability in this example was the incoherence between actual and accounted for physical passports and the MoI system.

Finally, the Kosovo case 4 (Falsification of tax documents) illustrates what happens when no one checks for a potential weak spot or link. In this case the owner of a company contracting with public institutions for cleaning services had used his "power" based on having good relations with tax officials. After one initial payment of a high-value tax, in all future bidding he had used the same receipt but with falsified dates. All officials of the institutions may request the original document, but they were reluctant to do so, as they felt they were dealing with a senior person, and provided the excuse that the document scanned met their requirements. However, no one checked, and as such this constitutes vulnerability. Here we are dealing with a case where officials could have safeguarded the procurement process by requesting the tax-document, but no one did.

Monitoring and auditing, as well as legal and procedural safeguards, should extend to and account for all systems and processes (electronic and physical) used by the public institution.

Vulnerabilities in outsourcing and IT contractor related risks

The Macedonian case 2 (Attack on the IT system for public procurement) represents an interesting case where an e-procurement system observes all possible technical safeguards, but becomes vulnerable to a distributed denial of service (DDoS) attack by being hosted in a shared environment with an ISP. Although the Macedonian authorities have not proven an abuse of official position and corruption, the case gives an overview of the procedure and potential methods of abuse of the IT systems for corruption, by abuse of official position or social engineering. The system administrator has full privileges into systems over a protracted period of time, and if his/

her activities are not appropriately controlled and monitored, he/she could abuse the system by destroying or altering the digital evidence, making it impossible to investigate the case and prove the abuse.

The Serbian case 2 (When IT contractor "takes root") represents the case where an IT contractor has an internal contact that manipulates data and procedures in favour of the contractor extending a favourable outsourcing contract. Procurement laws and regulations have since been amended in Serbia, but the disreputable employee exploited his knowledge of systems and requirements to favour a particular existing IT contractor in order to cut the contractor's expenses. He hid or made unavailable data regarding the IT contractor's access to the VPN WAN system and destroyed electronic documentation within the system so that the public institution (the MoJPA and later the new MoJ) could not control, monitor and supervise the system.

In the Albanian case 3 (IT corruption in the power distribution operator), the electricity distribution operator company was mostly privatised. Through an overbilling scheme, false readings from meter personnel's PDA devices, and in other cases allegations over electronic data having been altered in the company's IT system after they had been registered by the PDAs, overcharged customers electric bills. PDAs and procedures for meter readings initially were meant to ensure correct billing. But unauthorised entry and forgery of data, perhaps (but still not proven) even with help from the management, destroys whatever faith the public had in a fair meter reading process.

Finally, our collection of ICT corruption cases contains three examples of fraud and embezzlement in the road toll companies (Croatia case 8, Macedonia case 1, and Serbia case 4)[88]. In the case of Croatia and Macedonia road toll collection was outsourced to private companies, while in Serbia the company was fully state owned. Through schemes ranging from simple employee fraud in the Macedonian and Croatia cases, to an elaborate and more sophisticated scheme in the Serbian example, the risk of fraud and embezzlement is present where direct fee collection exists and where there is an inadequate monitoring of employees. In the Croatian and Macedonian cases the abuse was revealed through internal audit. In the Serbian case it was an internal whistle blower who revealed the abuse. In all three cases enhanced technical safeguards and monitoring of employees has later been implemented.

When ICT systems are outsourced, public bodies must in their contract with the IT contractor ensure that they are able to monitor and audit the systems

88 Croatia case 8 (Every year 2 million euros disappear from the tollbooths), Macedonia Case 1 (Abuse the IT System on pay tolls), and Serbia case 4 ("Road mafia")

not just in the same way as they would if it was an internal system, but to an even greater extent, as outsourcing generally implies a loss of control over systems.

Organisational and procedural safeguards

In Albania every government entity that revises or builds an information system must now get both a design review and receive no objection to the terms of reference from the experts in the National agency for Information society. Further, a system handover from contracting developer to public sector customer through an 'information system acceptance' procedure strives to ensure better integrity and quality of public sector information systems. In Bosnia and Herzegovina, the police IT systems and personnel working on these are now subject to regular checking by the competent authority. In Croatia under the Regulation on Information Security Measures, emergency planning procedures (development of procedures to follow in case of a security incident, and managing business continuity) is now stipulated. The Macedonian authors have observed a trend of signing non-disclosure agreements between economic operators and implementers where both parties agree not to disclose information for persons with system access. Further there is now an adopted practice in Macedonian institutions of separating the roles of technical administrators and content (data) administrators. Technical administrators are responsible for the system on an application level and managing users and access permissions. Content administrators for managing the data stored in the databases, but not the running of the systems themselves. In Montenegro, the Ministry for Information Society and Telecommunications have created several rulebooks to ensure standards, protection of data, incident management, content and manner of keeping records of certification of service providers, electronic signature, access to the eGovernment portal, and use the state organs internal network. Finally in Serbia, both the Ministry of the Interior and Ministry of Justice, have now implemented procedures regulating access to data to safeguard against abuse. Furthermore, in the Ministry of Justice nobody, not even high-level ranking employees, have access to data without prior approval from the court or prosecutors office.

Safeguarding through the 'many eyes' principle

Some examples from chapter 1 demonstrate 'simple' application of the 'many eyes' principles. For example, Croatia Case 5 (Policeman caught while inserting forged data in the police information system) where the head of the police station noticed the confirmation letter in the Ministry of the Interior information system, or the Macedonian case 4 (Misuse of registering working hours system) where a reassignment of tasks meant that a new administrator

had a look at the log files from the working hours system, thus performed a 'many eyes principle' auditing, and discovered the discrepancy.

In Croatia case 12 (You didn't spend a day of your life at work? No problem, you can still get a full pension!), the data consolidation in the OIB registry (OIB = Personal Identification Number) achieves the application of the 'many eyes principle'. While 'many eyes' could have been achieved in the Kosovo case 4 (Falsification of tax documents) had public officials in the various contracting government institutions just insisted on verifying the correctness of the tax document, the abuse would have been discovered much earlier and the procurement process could have been safeguarded through the 'many eyes' principles. The same lack of cross-checking holds true for the Montenegro case 3 (Abuse of functions and entering incorrect data in public registries) where edits in the municipal cadastre lacked organisational and procedural safeguards such as the 'many eyes principle'. No cross-checking was performed on the status of the land and ownership neither technically, nor by another employee in the municipal register, nor by an external audit.

Code of ethics

Perhaps as outcomes of the Croatian cases 9 and 10 concerning IT misuse by policemen, and the Croatia case 11 (Senior inspector misused confidential data to win the local elections!) a 'Code of Ethics' is instilled in public officials, and employees in the Ministry of the Interior and Ministry of Finance are obliged to act in accordance with it. What is equally important is that citizens can report civil servants' unethical behaviour to ethics officers.

Open data and government, letting the public help safeguarding data integrity and correctness

The Macedonian authors mention open government and open data as an example of anti corruption activities which enable citizens to take an active role in preventing and determining corruption. As such the 'many eyes' principle through citizen participation in scrutinising data, for instance final and property/asset status of high officials, can be enabled with opening government data. We know from a previous ReSPA study conducted in 2012[89] that at that time Croatia, Serbia and Macedonia were beginning to implement some initiatives around open data.

89 ReSPA Regional Comparative eGovernment Study (2012), available at: http://respaweb.eu/download/doc/Regional+comparative+eGov+study+-+web.pdf/dfab3d5a78e0d10e9-a6a80827e36a277.pdf

Training, ethics and integrity awareness

Albania now has an on-going initiative by the National Agency on Cyber Security in cooperation with the Albanian School of Public Administration organising training courses for almost all IT staff in public institutions. Training includes system security, protection, and risk evaluation. In Bosnia and Herzegovina there are now training modules for prosecutors in e.g. cybercrime and communication skills.

In Croatia the Regulation on Information Security Measures stipulates security awareness, as in establishment of safety rules and education for employees. Employees in the Ministry of the Interior are participating in various training and awareness raising projects on risks of ICT corruption and safeguards. The examples include two projects aimed at strengthening administrative capacities of the Ministry of the Interior in fighting cyber crime and a project on Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime. The project also includes workshops on networks forensic conducted by the Ministry of the Interior and the Croatian Academic and Research Network.

In Serbia the ministries of justice and interior now train their employees related to risks of ICT corruption.

In Macedonia the Public Administration Reform Strategy and Action Plan stipulates training and awareness for both civil servants and citizens on corruption. Montenegro offers user education in the field of information security and prevention of computer-security incidents.

Only Kosovo reports that there are no measures and no plans for offering training and raising awareness for civil servants on the risks of and safeguards against ICT corruption.

Whistleblowers

Some corruption offences will only be detected by internal sources who ´blow the whistle' on the true state of affairs. This is especially true if management is involved in the corruption. Kosovo case 4 (Falsifying the tax document) and Serbia case 4 (Road Mafia) illustrates how management and/or the whole organisation can disregard abuse of functions, fraud in office, embezzlement and organised crime, creating a culture where everyone is 'in' on the abuse, does not dare to do anything about it and accepts the situation, either because they are afraid of repercussions from revealing the abuse or because they benefit from it.

The human factor

Even if all ICT anti-corruption safeguards are observed, there is no guarantee that systems will not be abused. An illegal order from a manager to extract emails as in the Serbian case 3 (A senior public official spying on employees), or in the Albanian case 2 (Corruption in the Electronic Public Procurement System) where the majority of users become annoyed, especially with periodically changing complex passwords, and takes the shortcut to leave passwords unchanged with the default value that the system admin initially supplied them with at the first time login, will always exist.

Awareness amongst employees of the seriousness of compromising systems will be the key to secure and safeguard systems. This includes awareness not just of the security implications, but also of the ethical and integrity dimensions of civil servants work. Civil servants must be aware of both their rights and obligations, and the individual countries must establish modalities that support ethical behaviour.

Legislative safeguards

National authors list a range of legislative acts and national strategies covering areas such as: administrative procedures; electronic documents; classified information; electronic signature; personal data protection; public procurement; corruption and criminal code. It is outside the scope of this study to make a comparative analysis between each country's legislative safeguards, as they are included as contributions to illustrate legal safeguards relevant to the individual case examples.

An interesting lesson learnt from this study is the fact that there are cases where legal safeguards were inadequate for protection against ICT corruption.

The authors from Kosovo report that: "*in terms of administrative safeguards, Kosovo has adopted a set of laws, strategies and administrative instructions (normative acts) that relate to the usage of information and communication technologies, but the legislative infrastructure so far does not address properly the issue of data integrity and abuse of the information technology systems specifically or in general.*"

There are only a few case examples in this study describing inadequate legislative safeguards against abuse, and as such, lessons to be learnt. In the Macedonia Case 2 (Attack on the IT system for public procurement), the procurement rules seems not to take account of a situation where the

electronic bidding process is disrupted due to "technical" reasons. In another procurement example – Serbia case 2 (When IT contractor "takes root") – it was reported that the IT contractor had stopped the new tender process by utilising a complex and exhausting complaining scheme made available by the loopholes in the Law on Public Procurement. The law has since been amended ("Official Gazette of Republic of Serbia", no. 124/12).

In the Serbia case 1 (Sex at Belgrade Arena) internal administrative regulations were updated to include that: 1) unauthorised access to Ministry of the Interior data is now defined as not just a disciplinary, but a criminal offence; and 2) that the use of the data for any other purpose than the original one for why the data is collected is now defined as a criminal offence (not just disciplinary).

The case examples in this study are just examples. There is no representative information to draw any conclusion regarding general gaps in legislative safeguards.

3. Policy recommendations on mitigating corruption risks in ICTs

By Tilman Hoppe and Louise Thomasen

Part 1 – recommendations addressed at anti-corruption experts

Any stakeholder working on corruption prevention needs to accept ICTs not only as a tool for fighting corruption, but also as a risk for committing corruption. To this end, the following measures are necessary for **anti-corruption** experts:

1. Anti-corruption experts need to **cooperate** closely on identifying and preventing corruption risks from abuse of ICTs.
2. Corruption prevention bodies need to include the possibility of abusing ICTs for corruption into their catalogue of standard corruption risks. **Risk assessments** in public administration need to include the safety of IT against corruption risks. Risk assessments need to review any of the IT features listed below (Part 2 of the recommendations).
3. Heads of public entities as well as public officials need to be made **aware** of the risks which ICTs can pose with regards to corruption. Corruption prevention bodies need to actively offer advice on closing safety gaps in the IT of public administration.
4. Corruption prevention bodies and vocational training centres need to offer **training** on corruption risks connected to ICTs; such training should include IT experts.
5. National anti-corruption **strategies** and action plans should include a section on preventing corruption related to abuse of ICTs. If other strategies (such as on e-government or public

administration reform) already deal comprehensively with enhancing IT against abuse, the anti-corruption policy should at least contain a reference to the other strategies and ensure coordination between anti-corruption and IT experts on reform measures.

6. Law enforcement bodies and corruption prevention bodies should collect **statistical** data on IT corruption, analyse patterns, and adopt reform measures accordingly.

Part 2 – recommendations addressed at eGovernment experts

1. Access to all proprietary data and systems has to be safeguarded with **access control** using individual private user IDs and passwords.
2. In each public body it is a management responsibility to ensure that access to data is at the **appropriate level**. Access to proprietary data should be granted only when required for the immediate work tasks.
3. **Physical access** to facilities which store data or physical copies of data should be restricted to authorised personnel whose access is both logged and monitored.
4. Public organisations must implement **information security standards** such as ISO 27001 to ensure data safety and integrity.
5. **Disaster recovery and continuity plans** in case of security incidents should be developed for each public organisation. The plans must describe the procedures to follow in case of incidents, how to manage business continuity, and identify and agree on responsibilities for emergency arrangements.
6. All public organisations should implement **backup procedures** with periodic full backup of all systems and data. This includes desktop and laptop computers. Backup copies should be physically stored offsite.
7. **Log files** are a part of an organisation's monitoring and supervision structure. They also constitute an important auditing tool. Copies of log files should also be stored off site and/or separate from the application itself. Personnel responsible for altering content (data) should not be (technical) administrators of log files.
8. Public bodies must ensure that all their processes, regardless of their being physical or electronic, are not vulnerable to corruption abuse**. A compromised process or step in a process will influence all other** processes it interacts with. ICT systems that rely on input from other systems or processes are as safe from corruption as the systems and processes they interact with.

9. **Base registries** require special and heightened security measures as they are essential building blocks for coherent interoperable eGovernment.
10. **Outsourcing** IT development, maintenance, or deployment requires enhanced diligence by the public organisation that outsources. Responsibility can never be outsourced. When outsourcing, ensure that access to data is only possible for authorised assigned personnel, and that they are monitored and audited.
11. There should be a **separation of roles** between personnel responsible for data (content) and personnel responsible for systems (technology).
12. System **audits** and audit trails must never be monitored and administrated by the same IT administrator.
13. Supervision and applying the '**many eyes**' principle should be an integral part, not just in system design and development, but also in daily work.
14. Open government data and citizen participation in scrutinising public sector data can provide both 'reality checks' and improve data quality, as well as reveal irregularities and abuse. Also important in this context is providing the public with channels to give feedback to government and the public sector. In case of corruption/irregularities, ethics offices whom citizens can report civil servants unethical behaviour to can be such a channel.
15. It should be ensured that training on and raising awareness of ethics and integrity also includes personnel responsible for ICTs.

ReSPA is an international organisation which has been entrusted with the mission of boosting regional cooperation in the field of public administration in the Western Balkans. As such, ReSPA is a unique historical endeavour, established to support the creation of accountable, effective and professional public administration systems for the Western Balkans on their way to EU accession.

ReSPA seeks to achieve this mission through the organisation and delivery of training activities, high level conferences, networking events, summer schools, study tours and publications, the overall objectives of which are to transfer new knowledge and skills as well as to facilitate the exchange of experiences both within the region and between the region and the EU Member States.

CONTACT
Regional School of Public Administration
Branelovica
P.O. Box 31, 81410
Danilovgrad, Montenegro

Telephone: +382 (0)20 817 200
Internet: www.respaweb.eu
E-mail: respa-info@respaweb.eu