International Conference on Information Systems

University for Business and Technology - UBT

Proceedings of the 11th Annual International Conference on Information Systems

Edited by
Edmond Hajrizi

Leadership and Innovation

Education | Research | Training | Consulting | Certification

PROCEEDINGS

11th UBT ANNUAL INTERNATIONAL CONFERENCE

INTERNATIONAL CONFERENCE ON

Information Systems

29-30 OCTOBER

UBT Innovation Campus

Conference Book of Proceedings International Conference Pristina

ISBN 978-9951-550-85-7

International Conference on Business, Technology and Innovation Pristina, Kosovo 29-30

Editor: Edmond Hajrizi

Organizing Committee: Edmond Hajrizi, Hasan Metin, Visar Krelani, Hazir Cadraku, Retkoceri B, Selmani F, Muhamet Ahmeti, Selmani F, Muhamet Sherifi, Kastrati A, Mirlinda Reçica

Publisher, UBT

Editor Speech of IC - BTI

International Conference is the 11th international interdisciplinary peer reviewed conference which publishes works of the scientists as well as practitioners in the area where UBT is active in Education, Research and Development. The UBT aims to implement an integrated strategy to establish itself as an internationally competitive, research-intensive institution, committed to the transfer of knowledge and the provision of a world-class education to the most talented students from all backgrounds. It is delivering different courses in science, management and technology. This year we celebrate the 21th Years Anniversary. The main perspective of the conference is to connect scientists and practitioners from different disciplines in the same place and make them be aware of the recent advancements in different research fields, and provide them with a unique forum to share their experiences. It is also the place to support the new academic staff for doing research and publish their work in international standard level. This conference consists of sub conferences in different fields: - Management, Business and Economics - Humanities and Social Sciences (Law, Political Sciences, Media and Communications) - Computer Science and Information Systems - Mechatronics, Robotics, Energy and Systems Engineering - Architecture, Integrated Design, Spatial Planning, Civil Engineering and Infrastructure - Life Sciences and Technologies (Medicine, Nursing, Pharmaceutical Sciences, Phycology, Dentistry, and Food Science),- Art Disciplines (Integrated Design, Music, Fashion, and Art). This conference is the major scientific event of the UBT. It is organizing annually and always in cooperation with the partner universities from the region and Europe. In this case as partner universities are: University of Tirana – Faculty of Economics, University of Korca. As professional partners in this conference are: Kosova Association for Control, Automation and Systems Engineering (KA – CASE), Kosova Association for Modeling and Simulation (KA – SIM), Quality Kosova, Kosova Association for Management. This conference is sponsored by EUROSIM - The European Association of Simulation. We have to thank all Authors, partners, sponsors and also the conference organizing team making this event a real international scientific event. This year we have more application, participants and publication than last year.

Congratulation!

Edmond

Hajrizi, Rector of UBT and Chair of IC - BTI

Përmbajtja

Digital Transformation: A Review and Synthesis of the Literature

Njomza Mala[1], Melinda Pacolli[2]

[1]Njomza Mala Lushta, MSc candidate, ***Uninversity for Business and Technology, Prishtina, Kosovo***

(e-mail: nm64564@ubt-uni.net).

[2]Prof.Asoc.Dr.Melinda Pacolli, ***Uninversity for Business and Technology, Prishtina, Kosovo***

(ORCID: 0000-0001-7028-9952; e-mail: pacollimelinda@gmail.com).

Abstract: In recent years, there has been a steady increase in scholarly interest, which has resulted in a large rise in the number of articles covering various organizational and technological aspects of the digital transition. By sharing significant macro- and micro-level observations, we map the territory in this work and suggest future study directions for this broad topic. Our findings are primarily drawn from the literature on digital transformation. The literature search was performed on search engines such as Google Scholar, ResearchGate and Science Direct, for the period between 2001-2022. The report conducts a systematic analysis of 31 peer-reviewed studies that address various facets of digital transition, especially those related to cybersecurity and efficiency, that were published between 2001 and 2021. We extract additional analytical subunits for each dimension of DT that serves to separate the specifics of digital transformation processes and highlight the most significant and distinctive causes and effects that relate to digital transformation security.

Keywords: Digital Transformation, Information Systems, Technology, Digitalization, Digital innovation, Cyber Security, Information security, Sustainability, Challenges.

INTRODUCTION

Nowadays, the Digital Transformation is the bases for a successful business. A common key characteristic of all Digital Transformation initiatives is that they affect many organizational departments and processes, as well as external parties, such as customers or suppliers. Their main differences from more traditional IT initiatives are the complexity and cross-functional scope, the range of different stakeholders involved, and the extent of business and organizational changes needed to accommodate the new business models.

As a relatively researched topic, many peers have given different definitions for digital transformation. A tremendous power and consideration of digital transformation is that it can drive growth and innovation on every existing business existing today. Even different medical disciplines now are being renamed with the prefix digital. Digital transformation, smart technologies, and eco-innovation are paving the way toward sustainable supply chain performance. The connection between the digital transformation and human capital management is both undeniable and inescapable. The main posible drawback and challange for digital transformation may be the increased risk of cyber security, but this remains foreseen through collaboration with security specialists who are able to develop strategies and solutions to protect us from harmfull users and malware attacks. Findings are promising and this field requires frequent and continuous research to explore more connection and implication of digitalization.
Digital transformation is an 'evolutionary' process that involves integrating digital technologies into all aspects of an organization in order to improve operations, increase efficiency, and drive growth. While it presents challenges, the benefits it brings are numerous, such as improved customer experience, increased efficiency and drive for innovation.

Digital transformation is a vital change, which is determined by many factors. Some of the changes that imperatively impacts the digital transformation are the need for special technological and organizational resources, the creation of implementation strategies and the needs for trained human resources. Starting from the last point, the need for a trained staff determines the effect of digitalization, because digitalism requires human resources educated in the field of technology. The organizational structure of a unit that wants to implement a digital transformation must have a rich environment with technological tools, where through implementation strategies and trained staff it is put into operation. This conglomerate is a self-evident digital transformation, effective and, above all, can be a priority which will evolve in the future. The evolution aspect has a lot of value, because for technology there is nothing truer than it is updated every day, so we should keep following the latest changes and be updated too – just like a software.

METHODOLOGY

With this paper we aim to provide the latest information related to digital transformation and draw a series of conclusions, to understand digital transformation through the different perspectives, especially the security perspective.

This research study design is a review of the existing literature. The literature search was performed on search engines such as Google Scholar, ResearchGate and Science Direct. The search has also been extended through existing databases, e-Books and references cited in other relevant research. During search, a considerable number of peer-reviewed papers were collected, but only 31 of them were selected for systemic review. The selection criteria were made according to the year and place of publication, as well as the number of citations from other sources. All papers with a small sample, studies from countries with irrelevant research results and papers older that 2001 were excluded from the study.

The collected and reviewed material for this research is the most recent and updated and as a result we are aiming to provide findings on how to improve, reinforce and implement digital transformation. However, there is room for changes and new research opportunities, related to digital transformation, as a phenomenon present in many scientific fields.

DISCUSSION

The benefits that didigtalization brings to a business (alias company) are numerous, such as improved customer experience, increased work-efficiency and increased quality. Continuously investing in digital transformation would require continuously evaluate how digital transformation can improve (or is improving) their operations, and take steps to adopt in the processes for all the changes that are needed to achieve their goals.

Figure 1. Future of work framework – Digital transformation to bring in the new hyper age (Courtesy of **Sachin Mittal**

As a relatively researched topic, many peers have given different definitions for digital transformation. We would define digital transformation as an evolutionary phase of humanoid-activities using technology and Internet, towards offering a higher performance and effectiveness. Hinings et al., define digital transformation as the combined effects of several digital innovations bringing about novel actors (and actor constellations), structures, practices, values, and beliefs that change, threaten, replace, or complement existing rules of the game within organizations, ecosystems, industries, or fields (Hinings, 2018).

Digital transformation is the use of new digital technologies such as social media, mobile technology, analytics, or embedded devices to enable major business improvements including enhanced customer experiences, streamlined operations, or new business models (Kraus, 2018).

Businesses who are undertaking their own digital transformations, rethinking what customers value most and creating operating models that take advantage of what's newly possible for competitive differentiation (Berman, 2012).

Digital transformation can be understood both as a societal phenomenon and as a method for business development. We focus on the latter, the utilization of digital technologies by organizations in the establishment of new, digital value streams or how organizations use digital to transform from existing business models to newer ones (Magnusson, 2022).

Digital transformation is a subject working in four fields of activity related to the main internationalizing criteria. These are (i) costs, accessibility, resources and competencies; (ii) market knowledge; (iii) distance and location; and (iv) relational competencies and partner networks (Pereira, 2022).

Digital transformation can be comprehended as a continuous process of climbing the scale of digital maturity by employing digital and other technologies along with organizational practices to create a digital culture (Ivančić, 2019).

As we see above, there is a quite wide approach of businesses and research fields, towards digitalization. The rising importance of this topic, resulted in many findings through literature review but we conducted a categorized and well-structured scope of review and all the results are presented as digital transformation from the cyber security perspective.

RESULTS

We keep counting the positive aspects of digitalization, but we cannot forget the negative parts and challanges also. Have we ever thought of the security threats of our data, which

are stored somewhere “in the cloud”. It is officially confirmed that cybernetic security is the backbone of a successful digital transformation. Many digital platforms are in constant attack from botnets, bugs, SQL injections, PHP defacement, phpMyAdmin exploits etc., and that poses a great thread of data leakage or services impairement. Imagine a major hospital going offline due to an error in it's login system who is being breached by a newbie hacker somewhere in the third-world. That would pose a tromendous damage both in financial and human resources. Özsungur et al., in their book Business Management and Strategy in Cybersecurity for Digital Transformation illustrate how digital transformation show the importance of cybersecurity vulnerabilities. There is a major strategy development process against cybersecurity threats; sustainability elements in management; measures to be taken against cybercrime, cyberattack, and cyberterrorism; and organizational and business culture management in digital transformation (Özsungur, 2021). In literature review we noted that, there is a close cooperation between public and private actors is of central importance in the field of cyber security. In this context, the Alliance for Cyber Security alias ACS (in German, Allianz für Cybersicherheit), launched in 2012, who represents a successful model for creating cooperation between state and non-state (business) actors. The Alliance for Cyber Security offers its members up-to-date information on the IT security situation, various events for the exchange of knowledge and best practices, as well as a wide range of consulting and support services. Several thousand companies and institutions, such as the Federation of German Industries (BDI), have already joined the initiative - and the number is rising (Heckler, 2022). From our knowledge, a lot of private enterprises are now part of ACS, such as Kaspersky, WithSecure™, IBM® etc.

There are a lot of cyber security companies who offer protection against all harmfull attacks towards many digitalized innovations of our time. End-to-end encryptions are now the basis of making sure that you are not followed-up by a third-party. There are other good practices who are built upon voluntery basis, in order to perform a better security against threats. Such practices, usually known as Information Security Standards are COBIT (Control Objectives for Information and related Technology) and ISO 27000 Standards. This is just for the aspect of information security.

A recent survey found that 77% of IT decision-makers would have accelerated digital transformation sooner if they were aware of the full impact it could make on their organisation in just a few months. Now, 60% are accelerating the speed of their transformation projects as a direct result of the disruption the pandemic wrought on their workforces **(**Wilson, 2020). According to Forbes, 90% of the world's data was generated in the last two years with 2.5 quintillion bytes data being created each day (Marr, 2018). That’s what we call Big Data, but imagine the risk towards that amount of information shared everywhere. All those data came because of digital transformation to every business, even teaching, so we need them in order for our World to function better. As the aviation sector becomes digitized and increasingly reliant on wireless technology, so has its attractiveness to cyber attackers including nation-state actors and terrorists for example, vulnerabilities in the broad range of interconnected devices and (sub)systems, their implementations, as well as design flaws, can be exploited to carry out nefarious activities (Dave, 2022).

Just as natural disasters such as Earthquakes and tsunamis, cyber attacks are a threat to our time and reality. Imagine where would World be today without digitalization?! How long can you stay without your phone or smart watch, how harder it would be to diagnose a disease, how would you meet someone miles away from you etc. That’s why Nokia brought us a phone, iPhone brought us a mobile pone, Satya Nadella brought us Microsoft Teams and many more bright-minds are making sure to ease and digitalize us. But this doesn’t come without it’s consequences. Cyber security isn’t just the responsibility of software companies but ours also. No matter how secure a program is (for example e-Banking), if we fall in phishing fraud, we would enter a very high risk of lossing it all. So, if the Nigerian prince is asking for your help, ignore that e-mail, it’s just a phishing scam that is trying to lurk you into a trap of sending some money offshore.

Figure 2. The architecture of cyber security and different policies who are involvement in it both in governance, risk management, intelligence, analytics and reporting (Courtesy of **GBM** 8th Annual Security Survey 2019)

Opposing a real threat for digitalization, cyber security requires a lot of people involved in overcoming it. As seen in Figure 2, we show that there is a huge hierarchy of organizations and field-specific specialists who should work in collaboration and prevent the breaches of security. Issues with Big Data or Cloud Storage impairement are real threats of digital transformation. It's worth researching and improving further in this given subdiscussion of the digitalization topic.

BIBLIOGRAPHY

1. Hinings, B., Gegenhuber, T., & Greenwood, R. (2018). Digital innovation and transformation: An institutional perspective. Information and Organization, 28(1), 52–61. doi:10.1016/j.infoandorg.2018.02.004
2. Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital Transformation: An Overview of the Current State of the Art of Research. SAGE Open, 11(3), 21582440211047576. doi:10.1177/21582440211047576
3. Berman, S. J. (2012). Digital transformation: opportunities to create new business models. Strategy & Leadership, 40(2), 16–24. https://doi.org/10.1108/10878571211209314
4. Magnusson, J., Elliot, V., & Hagberg, J. (2022). Digital transformation: why companies resist what they need for sustained performance. Journal of Business Strategy, 43(5), 316–322. https://doi.org/10.1108/JBS-02-2021-0018
5. Pereira, C. S., Durão, N., Moreira, F., & Veloso, B. (2022). The Importance of Digital Transformation in International Business. Sustainability, 14. https://doi.org/10.3390/su14020834
6. Lucija Ivančić, Vesna Bosilj Vukšić, & Mario Spremić. (2019). Mastering the Digital Transformation Process: Business Practices and Lessons Learned. Technology Innovation Management Review, 9(2). https://timreview.ca/article/1217
7. Daniel Newman. (2018). Understanding the Six Pillars of Digital Transformation Beyond Tech. https://broadsuite.com/six-pillars-of-digital-transformation-beyond-tech/
8. Digital Adoption. (2022). What Are the 4 Main Areas of Digital Transformation?. https://www.digital-adoption.com/what-are-the-4-main-areas-of-digital-transformation/
9. Tonyushkina, K., & Nichols, J. H. (2009). Glucose meters: a review of technical challenges to obtaining accurate results. Journal of Diabetes Science and Technology, 3(4), 971–980. doi:10.1177/19322968090030044
10. Jenkins, C. (2023). Digital transformation meets evidence based medicine [Https://doi.org/10.1111/resp.14446]. Respirology, 28(2), 190–191. https://doi.org/10.1111/resp.14446
11. Jovičić, S. Ž., & Vitkus, D. (2023). Digital transformation towards the clinical laboratory of the future. Perspectives for the next decade. https://doi.org/10.1515/cclm-2023-0001
12. Patel, S., Goldsack, J. C., Cordovano, G., Downing, A., Fields, K. K., Geoghegan, C., … Robinson, E. J. (2023). Advancing Digital Health Innovation in Oncology: Priorities for High-Value Digital Transformation in Cancer Care. Journal of Medical Internet Research, 25, e43404. doi:10.2196/43404

13. Rehman Khan, S. A., Ahmad, Z., Sheikh, A. A., & Yu, Z. (2022). Digital transformation, smart technologies, and eco-innovation are paving the way toward sustainable supply chain performance [Doi: 10.1177/00368504221145648]. Science Progress, 105(4), 00368504221145648. https://doi.org/10.1177/00368504221145648
14. Alt, R., & Zimmermann, H.-D. (2021). The digital transformation of healthcare - An interview with Werner Dorfmeister. Electronic Markets, 31(4), 895–899. doi:10.1007/s12525-021-00476-1
15. Mair, F. S., Montori, V. M., & May, C. R. (2021). Digital transformation could increase the burden of treatment on patients. BMJ, 375, n2909. https://doi.org/10.1136/bmj.n2909
16. Latifi, R., Muja, S., Bekteshi, F., & Merrell, R. C. (2006). The role of telemedicine and information technology in the redevelopment of medical systems: The case of Kosova. Telemedicine Journal and E-Health : The Official Journal of the American Telemedicine Association, 12(3), 332–340. doi:10.1089/tmj.2006.12.332
17. Kuhn, S., & Jungmann, F. (2018). [Medicine in the digital age : Telemedicine in medical school education]. Der Radiologe, 58(3), 236–240. doi:10.1007/s00117-017-0351-7
18. Ekonomia Online. (2021). Rektori i UBT-së, Edmond Hajrizi renditet në mesin e personaliteteve botërore të dëshmuar në Extended Reality. https://ekonomiaonline.com/rektori-i-ubt-se-edmond-hajrizi-renditet-ne-mesin-e-personaliteteve-boterore-te-deshmuar-ne-extended-reality/
19. IPKO. (2017). IPKO tani mbulon 90 përqind të Kosovës me internetin 3G dhe 4G. https://www.ipko.com/ipko-tani-mbulon-90-perqind-te-kosoves-me-internetin-3g-dhe-4g/
20. Mardani A., Jabbour Charbel J.S.C., Cavallaro F., Deveci M. (2022) Digital transformation of human resource management: Current status, perspectives, challenges, and opportunities. https://www.emeraldgrouppublishing.com/calls-for-papers/digital-transformation-human-resource-management-current-status-perspectives
21. SME Portal of SECO (2022). Necessary resources for digital transformation. https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/necessary-resources-for-digital-transformation%20.html
22. Trenerry, B., Chng, S., Wang, Y., Suhaila, Z. S., Lim, S. S., Lu, H. Y., & Oh, P. H. (2021). Preparing Workplaces for Digital Transformation: An Integrative Review and Framework of Multi-Level Factors [Review]. Frontiers in Psychology, 12. https://www.frontiersin.org/articles/10.3389/fpsyg.2021.620766
23. Artemenko, E. (2020). The roles of top management in digital transformation. IOP Conference Series: Materials Science and Engineering, 940(1), 012014. https://doi.org/10.1088/1757-899X/940/1/012014
24. Fenech, R., Baguant, P., & Ivanov, D. (2019). The changing role of human resource management in an era of digital transformation. Journal of Management Information and Decision Sciences, 22(2), 166-175.
25. Strohmeier, S. (2020). Digital human resource management: A conceptual clarification [Doi: 10.1177/2397002220921131]. German Journal of Human Resource Management, 34(3), 345–365. https://doi.org/10.1177/2397002220921131
26. Pacolli, M. (2022). Importance of Change Management in Digital Transformation Sustainability. 21st IFAC Conference on Technology, Culture and International Stability TECIS 2022, 55(39), 276–280. https://doi.org/10.1016/j.ifacol.2022.12.034
27. Özsungur, F. (2021). Business Management and Strategy in Cybersecurity for Digital Transformation. In K. Sandhu (Ed.), Handbook of Research on Advancing Cybersecurity for Digital Transformation (pp. 144–162). IGI Global. https://doi.org/10.4018/978-1-7998-6975-7.ch008

28. Heckler, S., Klein, O. (2022). Cybersecurity: The backbone of a successful digital transformation. https://english.bdi.eu/article/news/cybersecurity/
29. Wilson, S. (2020). The pandemic, the acceleration of digital transformation and the impact on cyber security. Computer Fraud & Security, 2020(12), 13–15. https://doi.org/10.1016/S1361-3723(20)30128-7
30. Marr, B. (2018). Forbes: How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/
31. Dave, G., Choudhary, G., Sihag, V., You, I., & Choo, K.-K. R. (2022). Cyber security challenges in aviation communication, navigation, and surveillance. Computers & Security, 112, 102516. https://doi.org/10.1016/j.cose.2021.102516

Implementation of Anti-Covid-19 measures in Kosovo schools during October and December 2020

Bardha Qirezi [1][0000-0001-7294-7058], Rrita Cervadiku[2] [0000-0003-4919-7361]

and

[3]Diana Lekaj [0000-0001-8573-924X]

[1] UBT College, Kosovo

[2] Riinvest College, Kosovo

[3] UBT College, Kosovo

Abstract. The outbreak of Covid-19 imposed major restrictions across the globe including in Kosovo, necessitating adaptation of measures and plans that enable safe returning to schools and adequate response to further pandemic outbreaks. As such, in August 2020, the Ministry of Education and Science (MES) adopted guidelines for organising education in conditions of pandemics to be implemented by all schools using three available scenarios: Scenario A, physical presence with strict hygiene and social distancing measures limited to 20 students per classroom with at least 1,5 m distance, Scenario B: Combination of physical and online learning; Scenario C: Distance learning through TV and online platforms. This paper reports the adherence of schools to the MES Anti-Covid-19 measures from a monitoring process of 379 schools in 38 municipalities conducted from October to December 2020. The methodology used involved a site visit combining the interview with the management of the school using the checklist approved by MES and document analysis of evidence collected as foreseen in the checklist. The site visits were conducted in four phases according to a sample selected covering all 38 municipalities in Kosovo. The main results indicate a general mobilisation of schools to implement Anti Covid 19 measures especially regarding task force functioning, preventive hygiene measures and Covid 19 case reporting with difficulties in preparation and implementation of the learning process especially in scenarios B and C that involved distance learning.

Keywords: Covid 19 Measures, Kosovo, Pre-University Education

1. Introduction

In Kosovo, schools closed entirely from March 2020 to June 2020, resulting with an emergency distance education through public TV for grades 1 to 9 and ad-hock online learning integration mainly through zoom, google classroom, and Microsoft teams. According to Ministry of Education and Science (2020), around 9000 learners did not have means to follow TV classes or other online alternatives at all. While this number may be considered even bigger, the learning loss during the pandemics is a major concern for Kosovo. According to the report published in Spring by the World Bank (2020), the learning loss caused by school closures necessitated immediate response to prevent further risk to the already fragile human capital.

To mitigate the learning loss, MES exploring the model of scenarios used in Germany (Friedrich-Ebert-Stiftung, 2020), prioritised school reopening, necessitating urgent preparation of preventive measures and protocols. During July and August 2020, MES prepared the manual for the organisation of the learning process during pandemics with main aim to prepare schools, learners and parents for school reopening (Ministry of Education and Science, 2020). The Ministry of Education and Science Anti-Covid-19 measures aimed to ensure safer functioning of schools according to three scenarios: Scenario A, physical presence with strict hygiene and social distancing measures limited to 20 students per classroom with at least 1,5 m distance, Scenario B: Combination of physical and online learning; Scenario C: Distance learning through TV and online platforms. The scenario options depended on implementation of Anti-Covid 19 Measures and infection rates at schools.

The manual was consulted with health authorities, local governments and major actors in the education sector leading to a master plan approved by the Kosovo Government and additional budget to mitigate the Anti-Covid-19 measures required to reopen schools (The Government of Kosovo, 2020). Considering concerns regarding school infrastructure and hygiene prevention measures the implementation of the manual required additional time, budget and further organisation causing school reopening delay until 14th of September 2020. The main measures foreseen in the MES manual included: 1) Establishment of task forces at school, municipality and ministry level; 2) Preparation of schools for Covid 19 information, hygiene and social distancing measures, 2) establishing reporting Covid 19 cases and criteria for class or school closure; and 4) organisation of learning according to three scenarios; implying that students may move from one scenario to another depending on epidemiological situation. To ensure accomplishment of criteria for school reopening, a check list, provided in appendix 1, was approved by MES based on which MES inspections could judge accomplishment of criteria for school reopening and operation.

Given the importance for raising awareness for implementation of measures and for continuous monitoring, the researcher as part of Edutask in cooperation with Balkan Investigative Reporting Network (BIRN), a renowned media organisation, and with financial support from Friedrich Ebert Foundation (FES), conducted monitoring of implementation of Anti-Covid-19 measures in four rounds in 379 schools in Kosovo from 15 October to 15 December. After each round, a brief monitoring report was published highlighting the five most and least implemented measures and performance of schools and municipalities. In this report we present a general report on implementation of measures as well as brief recommendations for interventions and further research.

2. Methodology

The population for this study is 1094 schools in Kosovo at the preuniversity level as per the list of schools provided by MES (Ministry of Education and Science, 2020). The list includes

public and private preschools and nurseries, primary schools and lower secondary schools (grades 1-9) and upper secondary schools (grades 10-12). The list of schools provided by MES does not include schools which are not registered in the System for Managing of Education information (SMIA), excluding schools of the Serbian minorities administered by the Republic of Serbia.[1] A total of 379 schools were monitored during October and December 2020.

2.1. Sampling

Initially, stratified sampling was conducted based on which 79 schools were selected for monitoring in the first phase in October. With the interest to include more schools in the monitoring process, the sample was corrected and included 300 additional schools. Municipalities where the number of schools is extremely low have been included in the sample to include all municipalities in Kosovo. Subsequently, random sampling was conducted to select schools within municipalities, for the three more rounds of monitoring. The table 1 below shows the sampling procedure and the number of schools selected in each round according to municipality. The second monitoring was done in November and the third and fourth in December and each round included 100 schools.

Table 1. Sampling

Municipality	**Sample**	**Goal**	**Goal Correction**	**1st Round**	**2nd Round**	**3rd Round**	**4th Round**	**Total Monitored**	**Remaining**
Deçan	**2**	**8**	**8**	2	2	1	3	8	0
Dragash	**2**	**8**	**8**	2	2	0	4	8	0
Ferizaj	**4**	**16**	**16**	4	5	5	6	20	4
Fushë Kosovë	**1**	**4**	**4**	1	3	3	2	9	5
Gjakovë	**4**	**16**	**15**	4	5	5	6	20	5
Gjilan	**3**	**12**	**12**	3	6	4	5	18	6
Gllogovc	**2**	**8**	**8**	2	3	4	3	12	4
Hani i Elezit	**1**	**4**	**4**	1	0	1	2	4	0
Istog	**2**	**8**	**8**	2	3	3	3	11	3
Junik	**1**	**4**	**4**	1	1	0	0	2	-2
Kaçanik	**2**	**8**	**8**	2	3	2	1	8	0
Kamenicë	**2**	**8**	**8**	2	2	2	3	9	1
Klinë	**2**	**8**	**8**	2	3	2	3	10	2

[1] An exclusion is made in Kamenica where one school including Serbian minorities was monitored, although the school applied different regulation and therefore onlye measures applicable to them were monitored

Le-posaviq	**1**	**4**	**4**	1	0	0	0	1	-3
Lipjan	**4**	**16**	**15**	4	5	5	5	19	4
Mali-shevë	**3**	**12**	**12**	3	3	2	4	12	0
Mamu shë	**1**	**4**	**4**	1	1	0	0	2	-2
Mi-trovicë	**3**	**12**	**12**	3	5	7	4	19	7
Novo-bërdë	**1**	**4**	**4**	1	1	0	2	4	0
Obiliq	**1**	**4**	**4**	1	2	3	2	8	4
Pejë	**3**	**12**	**12**	3	6	6	5	20	8
Podu-jevë	**4**	**16**	**16**	4	5	4	6	19	3
Prisht-inë	**5**	**20**	**19**	5	7	16	0	28	9
Priz-ren	**6**	**24**	**23**	6	6	6	8	26	3
Rahov ec	**2**	**8**	**8**	2	3	5	3	13	5
Shtërp cë	**1**	**4**	**4**	1	1	0	2	4	0
Shtime	**1**	**4**	**4**	1	2	2	2	7	3
Skën-deraj	**3**	**12**	**12**	3	4	3	4	14	2
Suha-rekë	**3**	**12**	**12**	3	4	4	4	15	3
Viti	**3**	**12**	**12**	3	3	2	4	12	0
Vush-trri	**3**	**12**	**12**	3	4	3	4	14	2
Zubin Potok	**1**	**4**	**4**	1	0	0	0	1	-3
Zveçan	**1**	**4**	**4**	1	0	0	0	1	-3
Kllo-kot	**1**	**4**	**4**	1	0	0	0	1	-3
Ranillug		**0**	**0**	0	0	0		0	0
Partesh		**0**	**0**	0	0	0		0	0
Total	**79**	**316**	**312**	**79**	**100**	**100**	**100**	**379**	**67**

2.2. Data Collection

Data was collected by researchers[2] from BIRN Kosovo, which enjoys local and international recognition for fact checking[3]. The researchers used the check list for monitoring the application of Anti Covid 19 measures approved by MES (Ministry of Education and Science, 2020). The check list contains instructions on evidence to be gathered during school visits to judge the implementation of a measure. During the school visit, the researchers interviewed school management and asked for evidence foreseen in the checklist. The responses and evidence was registered online in the online platform shkollat.info (Edutask, 2020). The evidence data is visible for project staff, but not to the public, to meet ethical standards for data safeguarding. Although all data given by the school was given with permission, the platform shows only responses and comments of the researchers, and not actual documents and photographs. The platform choses 2 photos for each school to demonstrate some of the measures taken, mostly focusing on infrastructure.

As results are public, the schools were encouraged to write, comment and correct data, if they evidence that there was mis-judgment in the representation. If the school submitted such requests, the project leader conducted a quality check and responded to schools. In total only 5 quality checks and responses were processed during the monitoring phase.

2.3. Data Analysis

The check list contains three options for evaluation: 1) Fully accomplished, 2) Partially accomplished and 3) Not accomplished at all. One item within one measure category may contain one to three evidence checks. For data analysis, evaluation was given a quantitative measure. When one question or standard has three requirements, and one of three requirements are accomplished, the calculation is done as 50%, as ⅓ or 33% is calculated as 50%. Therefore, partial completion is evaluated with one or 2 requirements out of 3. Not accomplished at all is calculated as 0, when none of the requirements or evidence is completed within one item (0/3). Fully accomplished is calculated as 100, when 3 out of 3 requirements are accomplished. An average for each measure is calculated to show completion of measure, and the average of all four measures is calculated to show overall implementation of measures. It is important to notice that overall percentage reflects the average of four measures, although one measure may include more items than the other. Additionally, we must note that the first and the third measure is more technical, reflecting school reports and minutes to make judgments, whereas the second measure focuses on information, hygiene and social distancing measures that were more easily observed by researchers. The fourth measure was also based on management reports and researcher observations.

Firstly, the regional performance was evaluated, where the top performing and the low performing municipalities were spotted. Each of the measures was analysed to see which submeasures were more problematic for schools to fulfil, and which measures were mostly accomplished by schools. The tools which were used to analyse and visualize the data were Tableau and Excel. The results will be discussed further on in the paper.

2.4. Limitations

[2] 10 researchers from BIRN

[3] https://prishtinainsight.com/platform-receives-international-fact-checking-badge/

The school demographic data from MES was incomplete for the academic year 2020/2021, thus the monitoring could not include in the analysis demographic data for schools or show demographic data in the platform. In addition, school and MES data on infection rate is missing as it was not provided by the time this report is published. Additionally, according to the MES Manual, schools should have prepared for three scenarios, requiring schools to close for two weeks in risk of infection spreading and move to scenario C and afterwards return to scenario A or B depending on task force evaluation. The protocol that advised taskforces to close the class or school, was not consistent in all municipalities, and therefore the analysis is limited only in measuring establishment of the task force and its functioning without comparing school closing decisions.

3. Results

In this report, we report overall findings for four monitoring periods. In general, schools most of the times worked according to scenario A, moving to other scenarios depending on the epidemiological situation in the municipality and infection rates. The figure 1 shows the scenario adapted by the schools in each municipality during the monitoring time.

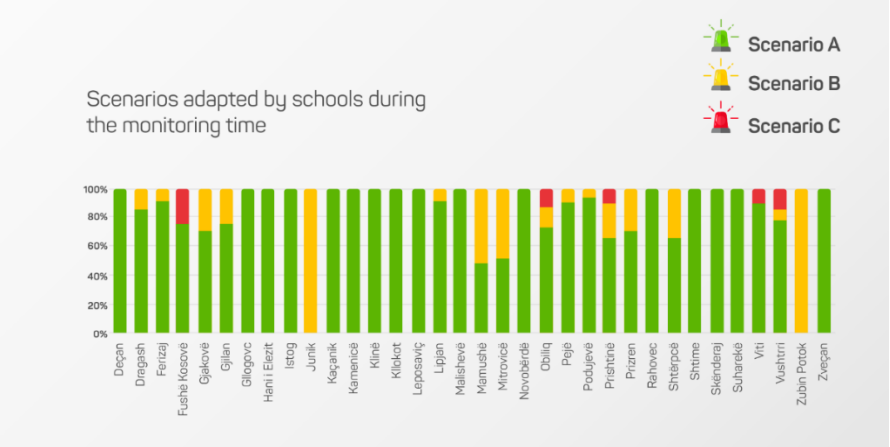

Fig 1. Scenarios adapted by schools during monitoring time

The average overall implementation rate of ant Covid 19 measures is 79.9 %. The highest implementation rate is reported for the measure 'Taskforce at the level of the institution (nursery/school)' at 88.7%, followed by ' Preventive Measures: testing, Covid 19 case reporting and school closure' at 81.5%, and 'Preventive Measures hygiene and protection – Preparing schools for beginning of the school year' implemented at 82%. Whereas the lowest rate is reported for the measure 'Organisation of the education process according to three scenarios in the MEST Manual' implemented at 67.7%.

Fig 2. Fulfilment of measures at national level

Further analysis of these measures presented in figure 3 shows highest average implementation rates at 95% or more for the following items: 'The taskforce at level of the institution is established ' and 'The school has prepared school schedule according to scenarios' (98%), 'Teachers are fully informed and participate actively ' and 'The task force is functional' (97.36%), `general school disinfection and thorough cleaning was organised',' active participation of teachers is ensured' and 'The school has temperature measurement equipment for regular usage ' (96%), 'The school has put posters for preventive measures against Covid 19' (95%).

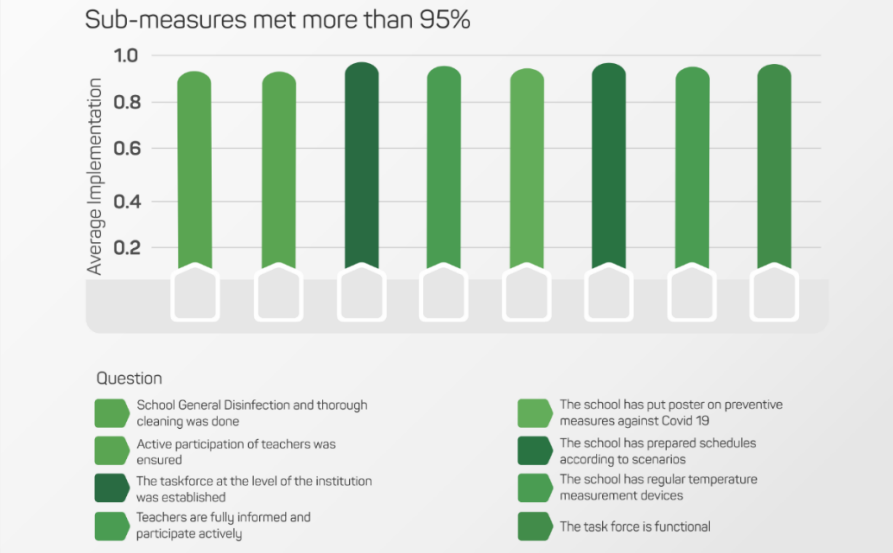

Figure 3. Sub-measures implemented at more than 95% at national level

The lowest implementation scores at 50% or less are observed for the following sub-measures at the national level: 'The training for students for the use of platform was conducted' (26.65%). ' MDA have ensured safe transport for specific groups of students ' (35.75%), The schools have allocated IT equipment for teachers ' and 'The school has secured IT equipment for learners ' ((37%), ' MED and Schools have secured additional technical personnel for sq m' and 'MED and schools have organised psychological counselling services ' (45%) , ' Schools have organised training for teachers to use online platforms ' (48.28%), 'MED and schools have prepared substitution list for teachers affected by covid 19'(49.87%).

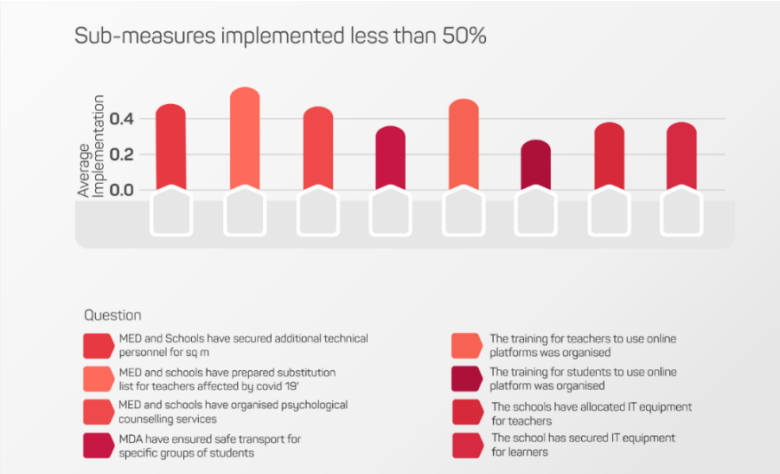

Figure 4 Sub-measures implemented less than 50% nationwide

Regarding the implementation of anti COVID-19 measures by schools by municipalities, from figure 5 we see that the municipality with the best performance is the municipality of Junik where the measures where fulfilled by an average of 94.9%, followed by the municipalities of Gllogoc (89.3%), Ferizaj (88.3%), Rahovec (87.25%), and Lipjan, Prizren, Skenderaj, and Gjakova implemented about 86% of the measures. On the other hand, the municipalities with the lowest performance of the implementation of anti-COVID-19 measures during this period include the municipalities of Leposavic and Shteepce where the measures were implemented only by 50.93% and 55.59% respectively.

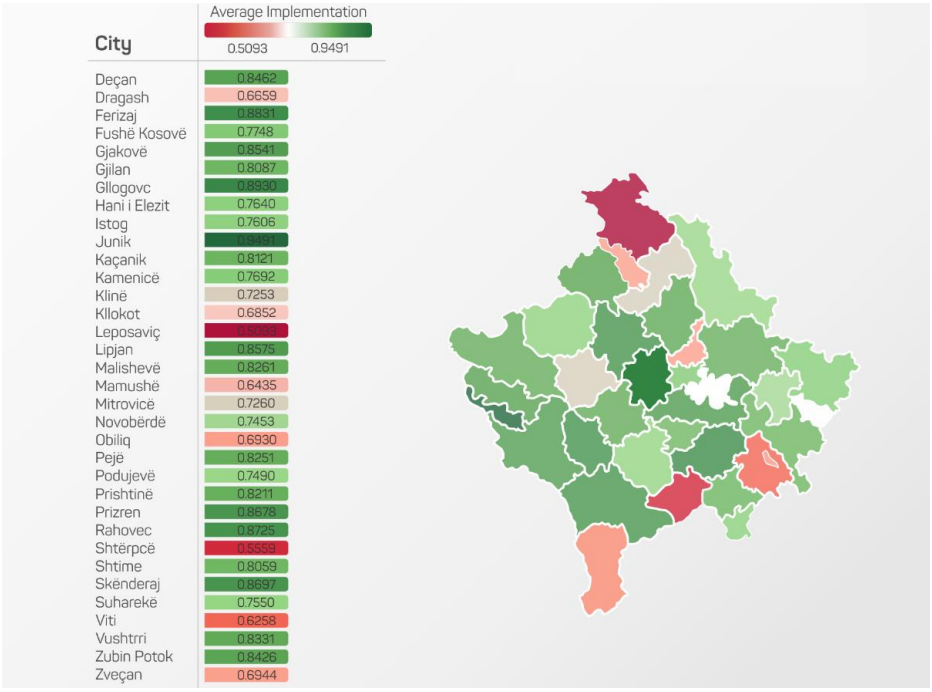

Fig 5 Implementation of anti COVID-19 measures in schools according to Municipalities

The data shows that in municipalities with Serbian majorities where two education systems work in parallel, the measures were least implemented mainly due to function of taskforces and lack of monitoring and coordination. The research did not include schools administered by the Serbian Education System and therefore the score according to the municipality only refers to schools administered by MESTI.

Figure 6 provides a more detailed overview of the fulfilment of each measure by municipalities. As it can be seen, all municipalities except the municipality of Leposavic have performed best in the implementation of the measure 'Taskforce at the level of preschool or school institution', from the four anti-COVID-19 measures. Regarding the implementation of preventive measures: testing, reporting cases with COVID-19 and interruption of education, most municipalities including: Junik, Deçan, Gjilan, Ferizaj, Gjakova, Gllogovc, Istog, Peja, Rahovec, Skënderaj, Prizren, and Vushtrri / Vuritrn have a very high implemention scores for this measure, whereas, the municipalities of Mamusha, Kllokot, and Shrërtrpce have not performed so well to

this extent. The municipalities of Junik, Gllogoc, and Zubin Potok have implemented quite well the measure of 'Hygienic and protective preventive measures - Preparing the school for the beginning of the school year'. Other municipalities have also performed quite well in implementing this measure, except for the municipalities of Shterpce, Leposavic and Zvecan. On the other hand, again the lowest performing measure out of the four measures imposed remains that of 'Organization of the learning process according to the three scenarios presented in the MES guide'. This measure received the highest score in the municipality of Junik and Prishtina and the lowest score in Viti, Dragash, and Shtrpce.

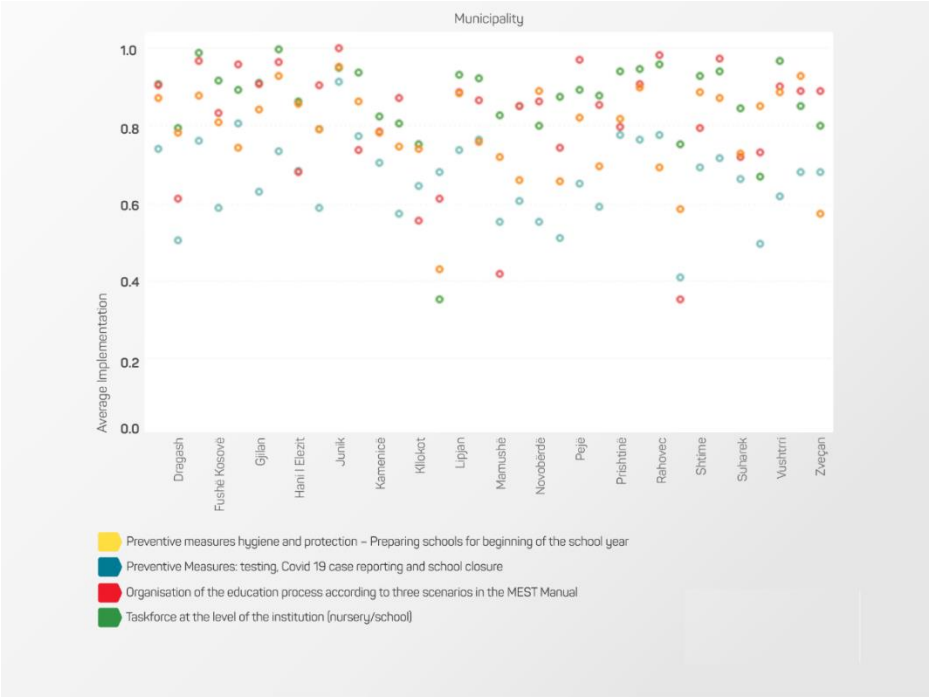

Figure 6. Fulfilment of anti-COVID-19 measures by measure type and municipality

4. Discussion

Results revealed three main systemic problems that affected implementation. First, although taskforces at school level were established and were functional, there were inconsistencies in monitoring and decision making at the level of municipal task force and coordination with MES task force. Task forces at school level, as newly established structures, were effective in managing implementation of preventive measures and making decisions about school closures based on the information collected at school. Secondly, although cases were reported in the official education management information system (EMIS), data were not monitored real-time at the level of MED and MES, mainly due low-level capacities for data analytics at municipal and central level. As a result, municipal and central government authorities could not predict infection rates and make consistent decisions across the schools. The infection spreading was mitigated by keeping contacts between groups minimal, and closing one class as soon as infection reported for two weeks, while keeping the rest of the groups in school, or moving to scenario B and C as necessary. Third,

schools could not employ substitute teachers due to employment restrictions although the government has approved the budget for this purpose. There were different approaches used by municipalities to employ additional teachers and technical staff. The least implemented measure was mainly concerned with the school capacity to organise learning in scenario B and scenario C, where there was evidence of limited capacities of school to organise online learning. While schools were successful to prepare instructions and organise schedule according to scenarios, they faced problems to secure equipment for teachers and students and to offer timely and effective training for students and teachers to use online platforms. Schools used different platforms (Microsoft teams, Google meet, Zoom) to organise synchronous lecture/meeting with students, lacking Learning Management Systems to upload learning materials and organise different learning activities including assessment. One of the main reasons for low implementation score for online platforms and distance learning was lack of unique digital systems and low digital competences among teachers.

5. Conclusion

Monitoring implementation of Anti Covid 19 Measures gives an overview of school efforts to respond to Covid 19 Pandemics and identifies areas that need to be improved. In 2020 schools in Kosovo mainly worked according to scenario A, organising classes with not more than 20 students, which made possible for safe returning to school, effective management of Covid 19 cases and mitigation for under preparedness to organise online learning. While schools responded effectively to preventive measures, they particularly faced problems with substituting teachers affected by Covid 19, organising effective training for students and teachers to use learning platforms, and providing adequate support and equipment to students when operating with distance learning. While, these results can be used to improve management processes and implementation of preventive measures, school, teacher and student digital capacities are harder to change in short term, and further research is needed to analyse the level of digitalisation in schools and digital competences among students and teachers, in order to increase the capacity to adapt to other scenarios if other school closures happen again.

6. References

1. Edutask. (2020). School performance Indicators Platform- Measuring the implementation of anti Covid 19 Indicator. Prishtina: Edutask. Retrieved from shkollat.info

2. Friedrich-Ebert-Stiftung. (2020). *Schools during the pandemic: Recommendations for organising the school year 2020/21.* Berlin: Friedrich-Ebert-Stiftung.

3. Ministry of Education and Science. (2020). Data set of preuniversity education institutions. (SMIA, Compiler) Ministry of Education and Science.

4. Ministry of Education and Science. (2020). *Lista e kontrollit per monitorimin e masave anti Covid 19 ne arsimin parauniversiatr.* Prishtina: Ministry of

5. Education and Science.

6. Ministry of Education and Science. (2020). *Udhëzues i përgjithshëm për organizimin e mësimit në vitin shkollor në kushtet e pandemisë Covid 19.* Prishtina: Ministry of Education and Science. Retrieved from https://masht.rks-gov.net/uploads/2020/08/udhezuesi-final-file-10-09-2020.pdf

7. Ministry of Education, Science and Technology. (2020). *The number of students excluded from distance education during closure.* Prishtina: Ministry of Education, Science and Technology.

8. The Government of Kosovo. (2020). *Master plani për zhvillimin e mësimit 2020/2021 në kushte pandemie.* Prishtina: The Government of Kosovo.

9. World Bank Group. (2020). *The Economic and Social Impact of COVID-19: Education.* Worl Bank Group. Retrieved from https://documents1.worldbank.org/curated/en/590751590682058272/pdf/The-Economic-and-Social-Impact-of-COVID-19-Education.pdf

Internal Security threats in Information System - threat protection at all stages of the chain

Amet Shabani*. Fatos Rushiti.**

University of Business and Technology UBT Pristina , 10000 Kosovo(amet.shabani@ubt-uni.net)

****University of Business and Technology UBT Pristina , 10000 Kosovo(fatos.rushiti@ubt-uni.net)***

Abstract: External threats are threats that come from outside the organization, where they are usually carried out by hacktivists from other countries, even competition. Common methods include ransomware, phishing attacks and hacking.

Insider threats originate from the organization itself and are usually carried out by a current or former employee, a contractor, a business associate, etc. Insider attacks can be malicious or unintentional. Common types of insider threats include unauthorized data transfer, abuse of employee privileges, and data sharing.

Insider threats have been a concern for organizations for a long time, but with digitalization and the growth of the network, they have become even more prevalent. Over the years, some of the largest and most expensive data breaches were caused by insider actors. The Tesla data theft case, which involved large amounts of highly sensitive data being transferred to unknown third parties by a malicious insider, clearly illustrates the danger of insider threats. Similarly, SunTrust Bank suffered a data security breach caused by an employee who stole the records of 1.5 million customers.

The goals of this paper are to identify vulnerabilities that consist of vulnerabilities in a system that can be exploited by attackers that can lead to dangerous impact.

This paper seeks to provide clarity on the different types of insider threats you should be aware of and the controls and processes that can be used to protect against them.

Keywords: Data, Internal Data Security, Internal Threats, Protection from Data Security Threats, etc.

1. INTRODUCTION

Whether they act as criminal or they neglect, insider threats pose a significant risk to all organizations.

Many different cyber threats targeting businesses,it's not always easy to know which part to prioritize. The mistake many organizations make is to focus solely on threats originating from the outside. However, with the continued increase in breaches caused by insider attacks, ongoing surveillance is required, and this can often be a very costly surveillance.

With the development of Information and Communication Technologies and increased access to the Internet, organizations become vulnerable to various types of threats. In fact, their information is exposed to cyber attacks and their damages. Threats come from various sources, such as: employee activities or hacker attacks. Financial losses caused by security breaches usually cannot be accurately detected, because a significant number of losses come from smaller-scale security incidents caused by an underestimation of the security risk of the information system. Thus, managers need to know the threats affecting their assets and identify their impact to determine what they need to do to prevent attacks by choosing appropriate countermeasures.

To find these threats, the sources of the threats and the specific areas of the system that can be affected must be known, so information security assets can be protected in advance. Thus, effective security classification is necessary to understand and identify threats and their potential impacts. In fact, security threats can be observed and classified in different ways taking into account different criteria, such as: source, agents and motivations. Threat classification helps identify and organize security threats into classes to assess their impacts and develop strategies to prevent or mitigate the impacts of threats on the system. There are several classifications and taxonomies of computer system attacks known in these papers. We note that many investigators have proposed taxonomies that classify attacks based on the intended effect of the attack such as denial-of-service attack, and others include the technique by which the attacker achieves this effect, such as: circumvention, authentication, or authority. The paper presents a hybrid threat classification model based on the combination of threat and impact classification techniques to better identify threat characteristics in order to propose appropriate countermeasures to reduce risks. The rest of the paper is organized as follows. The next section describes the principles of threat classification. In part 3, we present an overview of the most popular classifications of information security threats.

2. INSIDER SECURITY THREATS

Insider threats in cybersecurity are threats posed to organizations by current or former employees, contractors, business associates, or other partners. These individuals have inside information about the organization in question and can misuse access to the network, applications and databases to intentionally or unintentionally cause damage and disruption and/or delete, modify or steal sensitive data (Lindqvist U , Jonsson , 1997, pp. 154-163).

Information at risk of being compromised by insider threats can include personal information about employees and customers, intellectual property, financial data and details about the company's security controls. All organizations are at risk of insider breaches, but recent research has shown that the finance, manufacturing and healthcare sectors can be particularly susceptible (The Redscan Marketing team 2022).

According to the Kroll Global Fraud and Risk Report 2019/2020, incidents caused by insider threats account for 66% of those reported by organizations (Gordon LA, Loeb MP, Lucyshyn W, Richardson R, 2006).

2.2 Types of insider threats

Contrary to popular belief, insider threats are not always malicious in nature. Most definitions of insider threat include any action by an insider that can negatively affect an organization, and in many cases these actions arise from negligence rather than malice (Geric S, Hutinski Z., 2007, p. 31 -51).

Inadvertent insider threats often take the form of unintended employee mistakes, such as: falling for phishing scams or accidentally deleting files. Ponemon research has suggested that 63% of incidents related to insider threats in 2017 were the result of negligence (The Redscan Marketing team 2022).

Malicious insider threats include rogue and disgruntled employees or contractors who, in order to leak an organization's confidential data for financial gain, misuse access to systems to cause damage or disruption. Criminal insiders may work alone, collaborate with competitors, or be affiliated with organized hacking groups .

The four common types of insider threats are described below:

1. Second Streamers – Defined as current employees seeking to "stay and win," second streamers misuse confidential information to produce additional income through fraud, outside cooperation, or by selling trade secrets. Research by our Threat Intelligence team has found that cybercriminals are increasingly looking to target employees at large corporations, offering a payment for sharing credentials and further payments for each month they remain active.

2. Disgruntled Employees – Disgruntled current or former employees who steal intellectual property or commit deliberate sabotage are among the most costly threats to organizations. Gartner 's insider threat statistics suggest that nearly one-third of criminal insiders commit theft for financial gain.

3. Inadvertent Introverts – Inadvertent introverts are individuals who display confident and compliant behavior but make occasional mistakes and often do not realize their mistakes until it is too late.

The Persistent Irresponsibles – 4. The Persistent Irresponsibles are employees, often senior managers, who consistently do not attend cybersecurity awareness training. These employees often exhibit behaviors that can leave them vulnerable to compromise and are often targeted by social engineering scams such as: business email compromise (BEC) attacks (The Redscan Marketing team 2022).

2.3 Insider threat statistics: How big is the problem?

Insider threats are a growing problem, as evidenced by a recent Ponemon study "2020 Cost of Insider Threats: Global Report" (Tim Matthews , 2021):

• 60% of organizations had more than 30 internal related incidents per year.

• 62% of domestic related incidents are attributed to negligence.

• 23% of domestic related incidents are attributed to criminal insiders.

• 14% of internal related incidents are attributed to the theft of user credentials.

• The number of insider-related incidents increased by 47% in two years.

• Companies spend an average of $755,760 per internal incident.

Insider threats are difficult to detect because the threat actor has legitimate access to the organization's systems and data. This is because an employee needs access to resources such as e - mail , cloud applications or network resources to do their job successfully. Depending on the role,

some employees will also need access to sensitive information such as financial, patent and customer information.

Because the threat actor has legitimate credentials and access to the organization's systems and data, many security products would label the behavior as normal and not raise any alarms. Insider threats become more difficult to detect as they become more complex. For example, a threat actor may conduct lateral movements to cover its tracks and access high-value targets. Also an insider attacker could exploit a flaw in the system to escalate privileges.

2.4 Insider threats and privilege escalation

Insider attackers can implement their plans by abusing access rights. The attacker can attempt what is known as privilege escalation, which is taking advantage of system or application flaws to gain access to resources they do not have permission to access (Tim Matthews , 2021).

Figure 1 . Using privilege escalation, an attacker can move horizontally, gaining access to other user or service accounts, or vertically, gaining greater access through users

In some cases, abuse of access rights takes the form of someone with privileged access abusing their power. In 2008, a system administrator working for the San Francisco city government blocked access to the city's network and refused to hand over administrator passwords. The worker was unhappy and his job was at risk, but this was discovered (Tim Matthews , 2021).

These complex threats cannot be detected by traditional correlation rules because they are unknown threats. Instead, a security analyst would need to understand normal user activity to be able to identify abnormal and potentially malicious activity.

Table 1 . Insider threats are caused by malicious, negligent and compromised individuals whose motivations are quite different.

2.5 Internal threat motives

In most cases, the ultimate goal of an insider attack is financial gain, whether that's a malicious insider who has accepted money to provide confidential information, a negligent user who sends money to a bogus bank account after receives a fictitious or fake email , or a compromised insider whose credentials are stolen and used by attackers to exfiltrate and sell their patients' personally identifiable information (PII). In addition to the profit motive, there are many other motives for insider attacks, such as: sabotage, fraud, espionage, damage to reputation or professional gain. Insider threats are not limited to the exfiltration or theft of information, any action taken by an "insider attacker" that can negatively affect an organization falls under the category of insider threat.

Internal type	Motivations	Example	The danger
Criminal	Taking money or taking revenge on a light worker	Terminated employee plants logic bomb to execute malicious code	Theft of the main company's intellectual property. Disruption of operations. Damage to the company's reputation.

Negligent	Ignorance or carelessness	Careless employee publishes corporate data in public cloud space	Theft of the main company's intellectual property. Disruption of operations. Damage to the company's reputation.
Compromised	Oblivious to the danger they pose	An attacker uses compromised credentials to extort corporate data	Sensitive company systems or assets . Theft of the main company's intellectual property .

3. RISK OF BEING COMPROMISED

Insider threats in cybersecurity are threats posed to organizations by current or former employees, contractors, business associates, or other partners. These individuals have inside information about the organization in question and can misuse access to the network, applications and databases to intentionally or unintentionally cause damage and disruption and/or delete, modify or steal sensitive data (Lindqvist U , Jonsson , 1997, pp. 154-163).

Information at risk of being compromised by insider threats can include personal information about employees and customers, intellectual property, financial data and details about the company's security controls. All organizations are at risk of insider breaches, but recent research has shown that the finance, manufacturing and healthcare sectors can be particularly susceptible (The Redscan Marketing team 2022).

According to the Kroll Global Fraud and Risk Report 2019/2020, incidents caused by insider threats account for 66% of those reported by organizations (Gordon LA, Loeb MP, Lucyshyn W, Richardson R, 2006).

4.FREQUENT CASE OF THREATS

The results of the current research that I have drawn from the literature research provide unequivocal evidence that highlights the severity and prevalence of this threat in businesses today. According to a 2020 global report, the average global cost of insider threats increased by 31% in the past two years to $11.45 million , and the occurrence of incidents increased by 47% in that period. Through incident assessment and analysis, the insider threat (IT) challenge can be better understood and addressed. For example, the 2016 Threat Landscape Report from the European Union Agency for Cyber Security (ENISA) classified the top four insider incidents/actions as follows: privilege abuse (60%) (Observer IT , 2020), misuse of data (13%), use of approved device (10%) and abuse of possession of privileges (10%). According to the Threat Landscape Report 2018 by ENISA, 27% of data breach incidents were caused by human factors or negligence and according to a study, phishing (67%) is the main issue in the case of unwanted insider threats. Weak or reused passwords (56%), unlocked devices (44%), the practice of sharing passwords (44%) and insecure Wi-Fi networks (32%) were also on the list of unwanted insider threats . Furthermore, the report identifies that the prevalence of these attacks has increased to 56%, while 30% of organizations believe they have experienced an excessive attack.

This paper attempts to provide an informed assessment of the insider threat that is permanent and disruptive to organizations everywhere. Technologies and practices used by insiders are identified with explained relevance to the cyber attack chain. The practices that organizations should use to protect against insider threats are highlighted with shared best practices and recommendations to help combat the threat. In conclusion, a critical assessment of the relevant threat is presented, from understanding the nature of the threat to the best security defenses with the current

state of the art. A survey presents us with data from 105 enterprise users that reveal the insider threat arising from untrusted employees and inconsistent practices . However, the work does not highlight any breakthroughs or improved methods to combat insider threats. Further, a survey study considered only the three most common types of insider threats: traitor, masker, and unintended perpetrator, and discussed their countermeasures from a data analysis perspective. The work presents a detailed study on insider threats that decently summarizes the structural taxonomy of insider threat incidents. Their approach, however, focused on the relevant database and other aspects of internal incidents and their countermeasures

5. CONCLUSIONS

Security monitoring capability to prevent, detect and respond insider threats and other malicious activity require technology, intelligence and specialist expertise - which are very expensive.

In summary, the insider threat is still a real challenge for organizations. This work has investigated insider threats and their critical points for organizations to combat these threats and mitigate risk. Malicious insider attackers have become a major security issue for all enterprises as they can range from low-level employees to high-ranking personnel who have knowledge and access to confidential organizational information. Privilege escalation, exfiltration attacks, and APTs are some of the many techniques used by malicious insider attackers. To execute their attack, an insider attacker must complete all stages of the kill chain, so improving defenses at all stages of the kill chain can help stop future attacks. Improving protection can be done through the establishment of sound security policies and monitoring of employee activity that is essential in protecting against malicious insider activity. Thus, critical insider threat assessment serves as a tool for organizations to expand their knowledge of this ever-evolving threat. As previously mentioned, the different forms of internal threats must be addressed (detect the threat and prevent any inappropriate access to organizational resources), which target different subsystems of the organization, such as: device level, data, and corporate and business level.

ACKNOWLEDGMENTS

This work was supported by the University for Business and Technology UBT

REFERENCES

Yang, S.C.; Wang, Y.L. Insider threat analysis of case based system dynamics. Adv. Comput. Int. J. ACIJ 2011, 2, 1–17.
Liu, L.; de Vel, O.; Han, Q.; Zhang, J.; Xiang, Y. Detecting and preventing cyber insider threats: A survey. IEEE Commun. Surv. Tutor. 2018, 20, 1397–1417.
Homoliak, I.; Toffalini, F.; Guarnizo, J.; Elovici, Y.; Ochoa, M. Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Comput. Surv. 2019, 52
Gheyas, I.A.; Ali, E.A. Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. Big Data Anal. 2016, 1, 1–29.
White, S.J. Assessing Cyber Threats and Solutions for Municipalities. In Cyber-Physical Security; Springer: New York, NY, USA, 2017; pp. 49–65.
Nurse, J.R.; Buckley, O.; Legg, P.A.; Goldsmith, M.; Creese, S.; Wright, G.R.; Whitty, M. Understanding insider threat: A framework for characterising attacks. In Proceedings of the 2014 IEEE International Symposium on Security and Privacy Workshops (SPW), San Jose, CA, USA, 17–18 May 2014; pp. 214–228.
Haggard, S.; Lindsay, J.R. North Korea and the Sony Hack: Exporting Instability Through Cyberspace; AsiaPacific Issues 117; East-West Center: Honoloulu, HI, USA, 2015; pp. 1–8.

Gupta, S.; Kumar, P. Taxonomy of cloud security. Int. J. Comput. Sci. Eng. Appl. 2013, 3, 47–52.
Jaafar, F.; Nicolescu, G.; Richard, C. A systematic approach for privilege escalation prevention. In Proceedings of the IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Vienna, Austria, 1–3 August 2016; IEEE: New York, NY, USA, 2016; pp. 101–108.
Tsoutsos, N.G.; Maniatakos, M. Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation. IEEE Trans. Emerg. Top. Comput. 2014, 2, 81–93.
Giani, A.; Berk, V.H.; Cybenko, G.V. Data exfiltration and covert channels. Proc. SPIE 2006, 6201.
Clark, J.; Leblanc, S.; Knight, S. Risks associated with USB hardware Trojan devices used by insiders. In Proceedings of the IEEE International Conference on Systems Conference (SysCon), Montreal, QC, Canada, 4–7 April 2011; pp. 201–208
• Lindqvist U, Jonsson E. Si të klasifikohen sistematikisht ndërhyrjet e sigurisë kompjuterike. Simpoziumi IEEE për Sigurinë dhe Privatësinë; 1997. 154-163.
• Gordon LA, Loeb MP, Lucyshyn W, Richardson R. CSI/FBI Anketa e Krimit dhe Sigurisë Kompjuterike - 2006. Anketa e 11 -të Vjetore CSI/FBI për Krimet Kompjuterike dhe Sigurinë; 2006
• Omar, M. Insider Threats: Detecting and Controlling. In New Threats and Countermeasures in Digital Crime and Cyber Terrorism; IGI Global: Hershey, PA, USA, 2015; p. 162.
• Barrios, R.M. A multi-leveled approach to intrusion detection and the insider threat. J. Inf. Secur. 2013, 4, 54–65.
• Warkentin, M.; Willison, R. Behavioral and policy issues in information systems security: The insider threat. Eur. J. Inf. Syst. 2009, 18, 101–112.
• Greitzer, F.L.; Hohimer, R.E. Modeling human behavior to anticipate insider attacks. J. Strateg. Secur. 2011, 4, 25–26.
• Hunker, J.; Probst, C.W. Insiders and insider threats-an overview of definitions and mitigation techniques. J. Wirel. Mob. Netw. Ubiquitous Comput. Depend. Appl. 2011, 2, 4–27.
• Iyer, R.; Dabrowski, P.; Nakka, N.; Kalbarczyck, Z. Pre-configurable tamper-resistant hardware support against insider threats: The tested ILLIAC approach. In Insider Attack and Cyber Security; Springer: New York, NY, USA, 2008; pp. 133–152
• Kumar, G.P.; Morarjee, K. Ranking prediction for cloud services from the past usages. Int. J. Sci. Eng. 2014, 2, 22–25.
• Mihai, I.-C.; Pruna, S.; Barbu, I.-D. Cyber kill chain analysis. Int. J. Inf. Secur. Cybercrime 2014, 3, 37–42.

The impact of social media marketing on SMEs for the development of new websites in Kosovo

Agim Zuzaku [1][0000-0003-3811-9093]

[1] **University for Business and Technology, Pristina, Kosovo**

agim.zuzaku@ubt-uni.net

Abstract. The forms of marketing that SMEs can do online are wider and more comprehensive. Social networks are the platform that all businesses start their presence on the Internet because this is the most direct and fastest form of business-consumer communication. Therefore, this content should be carefully selected and different for different platforms. However, the website is and remains the identity card of an online business. The website is not that frequently updated, but it is the portfolio and history of that business. Therefore, SMEs whose main activity is mainly the sale and purchase of non-daily consumer products have an online presence. It is very important for SMEs to also be verifiable on Google as well as to be found positioned on online maps.
In recent years in Kosovo, we are seeing a decrease in the number of SMEs that are not developing their websites, while new companies are not investing in websites at all, focusing directly on social networks.
Through this research, we have identified the actual situation of SMEs in Kosovo that have websites and that do marketing on social networks, comparing the number of SMEs that do not have a website.

Keywords: Social Marketing, SMEs, Websites.

1 Introduction

The forms of marketing that SMEs can do online are wider and more comprehensive. Social networks are the platform that all businesses start their presence on the Internet because this is the most direct and fastest form of business-consumer communication.
Therefore, this content should be carefully selected and different for different platforms. However, the website is and remains the identity card of an online business.

From year to year, we have an increase in the number of users of social networks. In 2001 we had 1.482 million, while in 2022 we had 4.623 million. For each year, on average, we have a 12% increase in the population that uses social media. Around 59% of the world's population uses social media. The average daily usage is 2 hours and 29 minutes (July 2022) [1].

In the Western Balkans, which includes Kosovo, the use of the Internet in businesses is very prominent. From 2015 to 2019, almost 100% of enterprises in Serbia use the Internet for business. Enterprises use the Internet for business after Serbia, also at a high level they use it in Montenegro, then in Bosnia and Herzegovina. Albania from 2015 to 2021 has had an increase in the use of the Internet by about 2.2%, while only in 2021 the percentage of enterprises that used the Internet for business was 98.46%. Whereas, even though Kosovo is not far from other countries of the Western Balkans, based on the statistics from the statistics database that were generated only for 2018 and 2019, a decrease in the use of the Internet by enterprises is observed by 11% [2].

This rapid year-on-year increase in social network users has caused businesses to shift their marketing away from social networks, and most of them to give up on developing their own web pages.

1.1 Study Objectives

In recent years in Kosovo, we are seeing a decrease in the number of SMEs that are not developing their websites, while new companies are not investing in websites at all, focusing directly on social networks.

Study Objectives are to identifying the actual situation of SMEs in Kosovo that have websites and that do marketing on social networks, comparing the number of SMEs that do not have a website.

Research Question and Hypothesis. The research question of this study: Is social media marketing affecting the closure of websites, or the non-development of new websites of SMEs in Kosovo? The hypothesis of the study is Marketing on social networks has influenced the non-development of new SME websites in Kosovo.

2 Literature review

People spend a lot of time on the Internet, seeing the increasing interest of people in using the Internet, businesses have also moved to the Internet. Having a website with a presence on social networks has become the need of the hour. If you are a business owner and don't own a website, you could be missing out on a lot of potential customers online. Therefore, knowing the importance of a website is the key to growing your business exponentially [3].

Based on the review of the literature, many authors talk about the importance of web pages and social networks, but as a whole. Which means that SMEs must have a website with a presence on social networks. However, they do not treat it as a problem that has been present in recent years and SMEs are abandoning websites and staying only on social networks.

Fournier & Avery 2011, considering social networks, a salesperson must know every aspect of it. Social networks and the summary of social networks that connect to the Internet, applications that are built on the technological basis of Web 2.0 in consumer conversations enable brands to listen to consumer responses. presents an interesting point when they explain the difficulties for marketers in the Web 2.0 era. They emphasize their realization that social media was not made for brands, but for people. The days when the firm set the brand’s agenda is over and now

the consumers are the ones in charge. They decide when a brand can enter social communities [4]. Social networks offer a wide number of online alternatives, which make it more difficult for companies to know how to use them.

The advantage of the Internet marketing strategy is reflected in immediate communication, obtaining information from the right source, preparing and designing a product according to the wants and needs of the specific consumer, increasing direct sales, encouraging immediate purchase, as well as developing and maintaining the brand. A suitable website is a communication address with customers. A website is a tool with which the virtual company is realizing the goal of its marketing strategy and all the activities that are part of it. Companies that are not present on the Internet today are invisible to consumers. Therefore, the most effective marketing tool that companies should possess is the strategic planning of their online presence [5].

3 Research methodology

The study was conducted through quantitative methods. We have carried out desk research on social networks, identifying the companies that sponsor their ads, verifying them in the database of the Kosovo Business Registration Agency and researching whether they have a website.

We analyzed 384 SMEs, where we visited their page on the Facebook platform and then verified how many of them have active web pages.

Sample Size. We have used a sample calculation formula known as Cochran's Formula [6].

$$n > \frac{Z^2 \times p(1-p)}{e^2}$$

Z = Z value 95% => Z=1.96, (e.g. 1.96 for 95% confidence level)
p = percentage picking a choice, expressed as decimal (0.5 used for sample size needed)
e = confidence interval, expressed as decimal e=0.05 (e.g. 0.5=±5)

$$n > \frac{Z^2 \times p(1-p)}{e^2} = \frac{1.96^2 \times 0.05 \times 0.5(1-p)}{0.05^2} = 384.16$$

Minimum sample size would be 384 of businesses.

4 Results of the study

The majority of SMEs researched by activity are commercial and service enterprises.

Table 2. SMEs researched by activity

Types of SMEs researched by activity	
Construction	16.28%
Production	18.60%
Services	25.58%
Trade	39.53%
Grand Total	**100.00%**

According to the types of enterprises researched according to random methodology, about 40% of commercial enterprises, about 26% of service enterprises, 17% of manufacturing enterprises and 16% of construction enterprises responded to the research.

Table 3. SMEs researched by business registration

Types of SMEs researched by business registration	
Individual Business	20.93%
Joint Stock Company	6.98%
Limited Liability Company	72.09%
Grand Total	**100.00%**

Most of the researched SMEs according to the business registration are "Limited Liability Companies" enterprises.

About 68% of the surveyed SMEs have Facebook pages (Facebook page/Total)
About 32% have a website (Facebook page/Total).

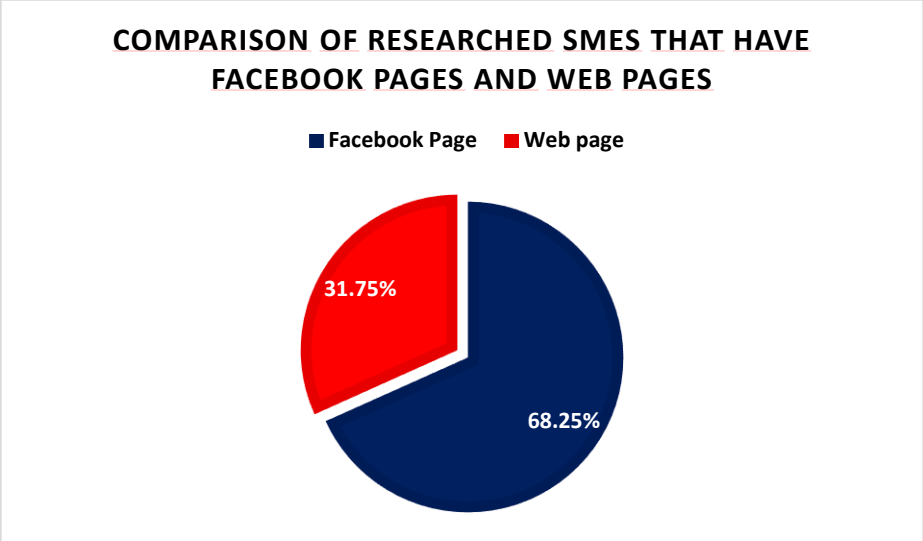

Fig. 7. Comparison of researched SMEs that have Facebook pages and web pages

While of the SMEs that have a Facebook page, 47% of the SMEs also have a web page. (Web page/Facebook page).

The majority of SMEs researched by activity are commercial and service enterprises (see **Error! Reference source not found.**).

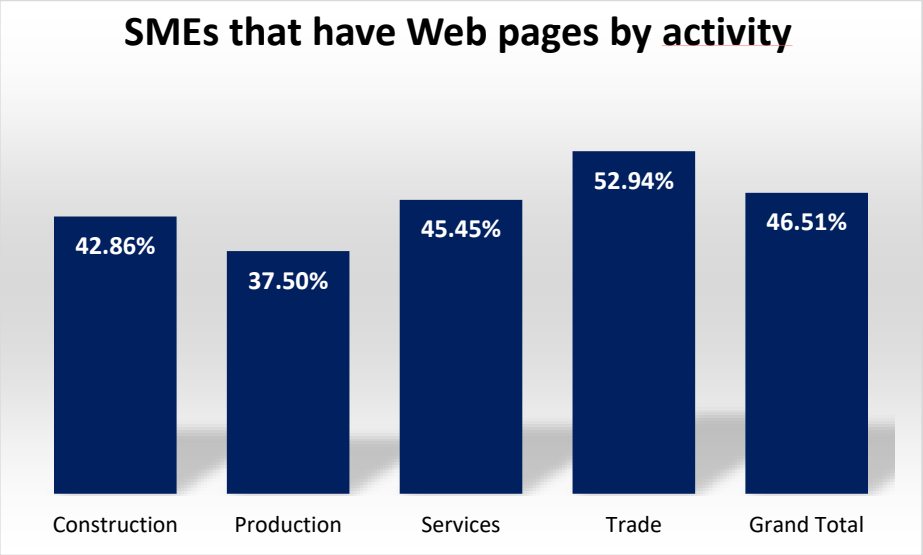

Fig. 8. SMEs that have Web pages by activity

About 48% of SMEs registered as Limited Liability Companies, in addition to Facebook pages, they also have active web pages. Only 22% of individual businesses have websites. Meanwhile, the Joint Stock Companies have 100% developed Facebook pages and web pages.

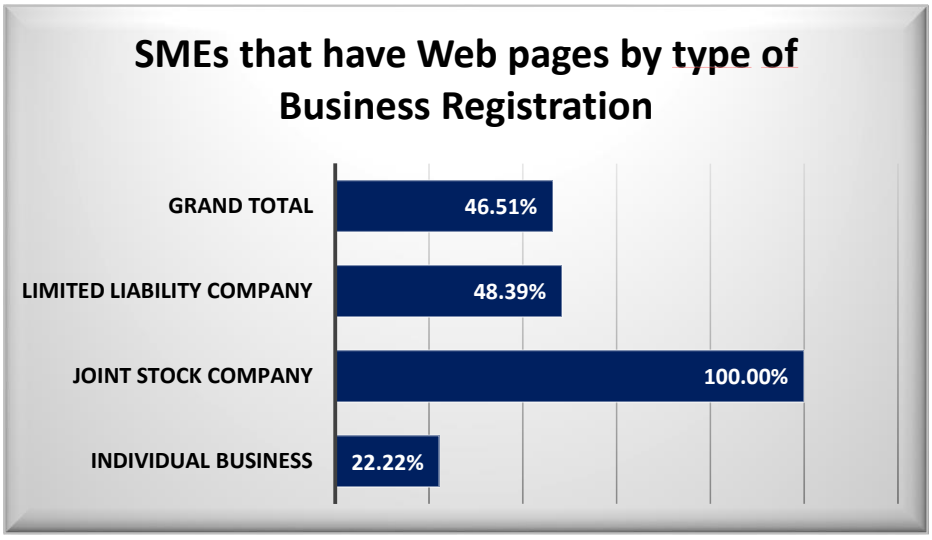

Fig. 9. SMEs that have Web pages by type of Business Registration

5 Conclusions

We can conclude that less than half of the researched companies have developed websites, which is a phenomenon that is increasingly growing in Kosovo. SMEs invest more in social media marketing than in website development. Whereas, the website is not updated that often, but it is the portfolio and history of that business. While from the literature we have noticed that in European countries websites are present on social networks, from this research we have noticed that now enterprises, especially small enterprises are increasingly present only on social networks.
SMEs should be present with their websites on social networks, this helps them to communicate more easily with their customers and have an address where customers can get complete information about the company and about the products or services they offer. they offer to their customers or clients.
Also, it is very important that SMEs are also verifiable on Google, as well as being positioned on online maps, because this makes them more visible to consumers in the case of their search in the search engine..

References

[1] D. Chaffey, "Smart Insights," Global social media statistics research summary 2022, 22 August 2022. [Online]. Available: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/. [Accessed 10 Decembar 2022].

[2] A. Zuzaku and B. Abazi, "Digital Transformation in the Western Balkans as an Opportunity for Managing Innovation in Small and Medium Businesses - Challenges and Opportunities," *IFAC-PapersOnLine,* vol. 55, no. 39, pp. 60-65, 2022.

[3] T. Ehsan, "Linkedin," Why Website is Important For a Business, 21 August 2021. [Online]. Available: https://www.infidigit.com/blog/importance-of-website/. [Accessed 11 Decembar 2022].

[4] A. Åberg, "BrandBa," HOW BRAND MANAGEMENT CAN SURVIVE THE WEB 2.0 ERA, 3 September 2015. [Online]. Available: http://www.brandba.se/blog/brand-management-web20-brandcommunity-bestpractise-airbnb. [Accessed 12 December 2022].

[5] S. Obednikovska, K. Sotiroski and E. Gjorgjioska, *ACADEMICA BRÂNCUŞI,* no. 3, pp. 82-91, 2019.

[6] W. G. Cochran, Sampling Techniques, Springdale, U.S.A.: John Wiley & Sons Ltd, 1963.

Using Machine Learning Tools to Study the Unemployment and Output Relationship in Albania

Blerina VIKA[1], Ilir VIKA[2], Kozeta SEVRANI[3]

[1, 3]Department of Statistics and Applied Informatics, Faculty of Economy, University of Tirana, Albania

[2]Research Department, Bank of Albania

blerina.vika@unitir.edu.al; ivika@bankofalbania.org, kozeta.sevrani@unitir.edu.al;

Abstract

The field of economics is nowadays increasingly employing artificial intelligence to complement and further improve the tools for analyzing and making future decisions. One of the most common machine-learning techniques that are used in forecasting economic indicators is the recurrent neural network method, which has often proven to be useful in capturing non-linearities in data series. This article applies the long short-term memory (LSTM) technique to test for the Okun relationship in Albania. Apart from examining movements in unemployment as predicted by developments in aggregate demand, we test whether a disaggregated version of the Okun's law – by decomposing aggregate demand into various expenditure components of GDP – provides better predictions for changes in unemployment. In-sample estimations suggest that the Okun's law may hold in Albania, but the response of unemployment to output performance is found to vary over different time periods. Non-linear model forecast evaluations show that unemployment rate movements in the second half of 2010s could be more related to private investment and government spending, while private consumption and external trade developments seem to predict it less.

Keywords: Machine Learning, LSTM model, unemployment, Okun relationship, Albania.

Disclaim: This research article is considered as a preliminary work that aims at stimulating debate and critical comments. It expresses the views of the authors and does not necessarily represent those of the institutions where they work. The authors are grateful to comments and suggestions received from participants at the "11th International Conference on Business, Technology and Innovation 2022", organized by the University for Business and Technology - UBT, Pristina, Kosovo, in October 29-30, 2022.

1. Introduction

There is a general consensus today that inequitable economic growth might have adverse effects in the society. For that reason, governments around the globe have increased their awareness on the importance of inclusive growth and are pushing their political agenda to make sure that economic growth could deliver more jobs and promote higher living standards for their citizens. Emerging and developing economies have been growing rapidly for a number of decades. Yet, recent empirical findings reveal that their satisfactory performance has been in the large part not necessarily translated into more employment and equal opportunities.

This paper uses the Okun relationship to examine movements in unemployment as predicted by developments in aggregate demand in Albania. In addition, it test whether a disaggregated version of the Okun's law – by decomposing aggregate demand into various expenditure components of GDP – provides better predictions for changes in unemployment. The hypotheses are tested by using the econometric least square method as well as a rather novel technique in this regard by employing the long short-term memory (LSTM) model. The latter is a machine-learning technique that has often proven to be useful in capturing non-linearities in economic data series.

To preview the results, the OLS estimations appear to be in favor of the Okun relationship in Albania. Estimating different sub-samples suggests that the response of unemployment to output could be time-varying, while faster domestic growth may be needed to keep unemployment rate from rising. On the other hand, the preliminary results in this ongoing project show that adding output growth to the LSTM forecast model does not improve the unemployment predictions that are generated from a univariate model. Nevertheless, the LSTM model predictions with GDP components reveal that unemployment could be more related to private investment and government spending, and perhaps not so much linked with private consumption and external trade.

The remainder of the article is organized as follows. In section 2 we provide a glimpse at the empirical literature on unemployment and growth in advanced and developing countries. Section 3 estimates the Okun coefficient in a simple OLS regression to examine the contemporaneous relation of unemployment with aggregate demand in Albania. In addition, to shed light on the stability of their relationship, the Okun coefficient is estimated for i) the early transition years, ii) the faster growth period, and iii) the post-global crisis decade. Section 4, then, reassesses the relevance of economic growth in the Okun relationship by relying on the information embedded in GDP and its expenditure components to improve upon the benchmark univariate forecasts of the unemployment rate. Moreover, as the in-sample estimations in section 3 evidenced a time-varying Okun coefficient, the uncommon cross-checking analysis in section 4 is based on the nonlinear LSTM model. The concluding remarks are available in section 5.

2. A brief literature review

Despite some theoretical limitations of Okun's law, Prachowny (1993) and Blinder (1997) conclude that Okun relationship is a useful principle of macroeconomics in which 'we should all believe'. In his seminal paper on the relationship between GDP developments and changes in unemployment, Okun (1962) originally treated unemployment as the exogenous variable while output as the dependent variable. However, the rich empirical literature estimating the Okun relationship has been mostly interested in the reverse direction, hence assuming the output growth as the driving force of unemployment.

The link between unemployment and output is generally assessed by transforming the variables in gaps or in differences. The "Gap" version relates the divergence of current unemployment (U_t) fromt its "natural" rate (U^*) with the deviation of actual output (Y_t) from its potential level (Y^*) [$U_t - U^* = \beta(Y_t - Y^*) + \varepsilon_t$]. On the other side, "Difference" version relates changes in unemployment rate to economic growth [$\Delta U_t = \alpha + \beta \Delta Y_t + \varepsilon_t$], thus assuming that the "natural" rate of unemployment is zero [$\Delta U^*=0$] while potential GDP growth is constant [$\Delta Y^*=g$].

The original Okun's paper estimated that β equaled negative 0.3 in the U.S. during the 1947-60 period. However, the recent empirical literature on the Okun's law has found heterogeneous evidence with respect to the size of the Okun coefficient. The difference among countries might have much to do with the very definition of unemployment, as the term does not follow a worldwide standard definition of measuring employment, nor can data availability be comparable between formal and shadow economies. Also, labor market rigidities and government social protection policies on employment have often been emphasized when trying to explain the heterogeneous sensitivity of unemployment to output decline, particularly among advanced economies [see e.g. IMF, 2010; Cazes, Verick, & Hussami, 2013].

A review by Pizzo (2019) shows Okun's coefficients in rich economies as estimated with the difference (gap) version are around -0.29 (-0.39), while in developing and emerging market economies they are -0.18 (-0.20). Other studies have similarly concluded that unemployment is less sensitive to production in developing than in advanced economies [see e.g., Ball et al., 2019; An et al., 2017; Bartolucci et al., 2018]. Using a sample of 176 countries for the period 1993 until 2015, Farole et al. (2017) evidence that Okun's coefficient is not constant across countries. For every percentage point increase in GDP, unemployment rates would decline on average for the high income, upper-middle income, lower middle-income, lower income countries by 0.21, 0.08, 0.03, and 0.005 pp, respectively.

Furthermore, reassessments after the Global Crisis period indicate that Okun coefficients all over the world have declined when comparing the pre-crisis (1992-2007) with the post-crisis (2010-2017) period (Lee et al., 2020). Yet, Farole et al. (2017) find that in transition economies like Ukraine and Croatia unemployment seems to react asymmetrically over the business cycle: the size of coefficients show relatively strong reaction during downturns, but much weaker upside response during periods of upward growth.

Using only the "difference" version and running pooled OLS for ILO data sets on unemployment, Lee et al. (2020) find that during the 1992-2017 period the Okun's coefficients are -0.22 in twenty nine NSW European countries and -0.15 in ten Eastern European economies. Anyhow, Farole et al. (2017) find a large difference among similar income countries in CE Europe. For example, the Okun coefficient is estimated 0.85 in Poland, but just 0.03 in Hungary. In Albania, Garo (2020) finds that "for a 1 p.p. drop in the output growth, the annual change in the unemployment rate increases about 0.184 p.p. over 4 consecutive quarters".

3. Does Okun's law hold in Albania? An OLS approach with aggregate demand

The link between unemployment and output is typically examined by assessing their contemporaneous relationship:

$$\Delta U_t = \alpha + \beta_y \Delta Y_t + \varepsilon_t \qquad (1)$$

where ΔU denotes annual change in unemployment rate; ΔY is annual growth rate of output; α is an intercept coefficient that captures the trend growth in unemployment rate ($\alpha = - \beta \Delta Y^*$); β is the so-called "Okun coefficient", denoting the sensitivity of unemployment rate to GDP growth, which is expected to be negative, since a higher GDP growth rate should lead to lower unemployment rate; ε is an error term.

We test for the Okun relationship using quarterly data from 1996q1 to 2019q4. As Albanian economy has experienced significant fluctuations during this period, it may be possible that the correspondence between variables be both nonlinear and time-varying. Thus, we test for changes in the Okun relationship during the i) early transition period of 1996q1-2003q4; ii) fast economic growth from 2003q1-2010q4; and the post-global financial crisis decade from 2011q1-2019q4.

Table 1. Okun coefficients for Albania: aggregate relationship

Table 1. Okun coefficients for Albania: aggregate relationship

	(1) Full Sample 1996q1:2019q4		(2) Early Transition 1996q1:2003q4		(3) Fast Growth 2003q1:2010q4		(4) Post-Global Crisis 2011q1:2019q4	
Dependent Var. ΔU	Coef.	Prob.	Coef.	Prob.	Coef.	Prob.	Coef.	Prob.
ΔY (βy)	-0.090***	0.00	-0.075*	0.10	-0.212***	0.00	-0.581***	0.00
Constant (α)	0.236	0.23	0.436	0.28	0.820***	0.00	1.182***	0.01
Adj. R-squared	0.07		0.06		0.54		0.32	
Included observations	96		32		32		36	
Ratio of -α/β	2.6		5.8		3.9		2.0	

Table 1 displays the estimated Okun coefficient for the aggregate relationship in Albania. The estimated response of unemployment to output growth is statistically significant and has a negative sign as expected, hence suggesting a well-functioning labor market. The Okun coefficient, β, is, however, not constant and appears to have considerably increased in magnitude over time. The relationship is estimated to be modest in the full sample (-0.09). The result is in line with the findings from Farole et al. (2017) for middle-income countries, which are often characterized by insufficient safety nets and relatively large share of self-employed workers. However, the relatively low reaction seems to be influenced by the early transition period. Later on, the size of β coefficient increases significantly and implies a relatively significant job creation in the post-GFC period (-0.58). But, so has the trend growth in unemployment rate as captured

by the intercept parameter, α; in the last period in column (4) is about 5 times higher than for the full sample, hence well above the assumption of zero changes in the "natural" rate of unemployment. Finally, the time-varying parameters are reflected in a declining ratio of model coefficients ($-\alpha/\beta$) – found to be statistically significant since 2003 – which may imply that the Albanian economy needs to grow faster in order to leave the unemployment rate unchanged.

4. Decomposing the Okun's law: do expenditure components enhance prediction ability?

Methodology

The vast empirical literature on the Okun relationship evidences that economists widely believe on the existence of a long-run relationship between GDP performance and unemployment. Yet, the short-run dynamics may disguise the long-run bond between the variables. The previous section revealed a rather time-varying Okun relationship in Albania, suggesting a lack of stability in the coefficients over the past two and a half decades.

To shed more light on the suitability of Okun's law as a "rule of thumb" for predicting unemployment rate, certain studies have resorted to analyses that decompose the Okun relationship into expenditure or production components. We follow them by decomposing here the aggregate demand into private consumption (con), public expenditure (gov), private investment (inv), exports (exp) and imports (imp).

Furthermore, the mainstream studies have commonly relied on traditional econometric models to estimate and test the stability of the Okun coefficient. In contrast, we follow a novel approach to test for the Okun relationship by relying on unemployment predictions generated by nonlinear nonparametric Machine Learning (ML) methods. These innovative techniques could be suitable in resolving possible issues of nonlinearity and time-varying relations in our variables, due to changing domestic and external economic conditions. Among the wide class of these techniques, we have selected to apply in our analysis the long short-term memory (LSTM) model. This method belongs to the artificial recurrent neural network family, which have gained popularity in the area of artificial intelligence and deep learning. Moreover, machine learning methods are nowadays being seen as a new exciting 'car' on the street by many central bank economists, who are increasingly experimenting with ML techniques as additional supporting tools to help improve economic forecasts and monetary policy decisions. Unlike the feedforward neural network that we have experimented before (e.g., Vika & Vika, 2021), the recurrent neural network LSTM has feedback connections and is capable of learning long-term dependencies. Once we train and test the LSTM network structure, we use the out-of-sample forecasts computed by it to assess the relevance of economic growth in the Okun relationship by relying on the information embedded in GDP and its expenditure components to improve upon the benchmark univariate forecasts of the unemployment rate.

Data and forecasting procedure

All variables are seasonally adjusted by using the X-13 ARIMA-SEATS procedure in EViews software. The whole sample period covers quarterly data from 1996Q1 to 2019Q4. Each model includes three lags as inputs of each variable, as suggested by Akaike and HQ info criteria in the estimated least squared regressions. Forecast evaluation is undertaken for out-of-sample forecasts, using the RMSE measure for a forecast horizon of 4 quarters. In our analysis, the 1996Q1:2019Q4 period has been divided into the so-called training period 1996Q1:2014Q4 (76 quarters) and the forecast evaluation period stretching over the 2015Q1:2019Q4 sample (20 quarters).

Consequently, the model starts for the period 1996Q1:2014Q4. For each specification the forecast and its corresponding RMSE is noted down for the 4 quarters ahead. The training and testing period is recursively extended by one quarter (1996Q1:2015Q1), and similarly calculating and retaining the RMSE of forecasts for the desired one-year ahead horizon. The evaluation process is repeated 16 times for the 4 quarters horizon until we predict the last quarter of 2019.

Forecast evaluation results

Table 2 displays the forecast gains/losses in using GDP growth and its expenditure components to predict changes in the unemployment rate. A ratio above 1 indicates underperformance of the bivariate LSTM networks. It turns out that including GDP in the unemployment LSTM model does not outperform the latter's forecasts that are based on its own past values. The ratio of RMSE is just above 1, casting doubt on the predictive content of output growth on unemployment rate. However, the evaluation of loss differentials for individual expenditure components reveals some interesting results on the effectiveness of this approach with the aggregate relationship. The RMSE ratios for government spending (0.84) and private investment (0.81) suggest us that these expenditure components could be the key factors in delivering jobs and relieving unemployment in Albania. On the other hand, private consumption (1.15) and external trade (1.07) seem to have no predictive power on the rate of unemployment.

Table 2. The loss differential between forecasts, 2015q1:2019q4, h=4 quarters

Table 2. The loss differential between forecasts, 2015q1:2019q4, h=4 quarters

Bivariate Models:	Δu-Δy	Δu-Δcon	Δu-Δgov	Δu-Δinv	Δu-Δexp	ΔU-Δimp
Ratio of average RMSE: (Bivariate/Univariate f'casts)	1.01	1.15	0.84	0.81	1.07	1.07

5. Concluding remarks

The results from OLS estimations seem to be in favor of the Okun relationship in Albania. The coefficient is found to be rather low for the past two and a half decades, in line with other studies for low and middle income countries. Estimating different sub-samples shows considerable lack of constancy in the coefficients that measure the sensitivity of unemployment to output as well as the trend growth of unemployment. Yet, faster domestic growth may be needed to keep unemployment rate from rising. Moreover, LSTM forecasts indicate that unemployment could be more related to private investment and government spending, while private consumption and external trade developments do not seem to improve upon the univariate forecast accuracy.

While social demographic changes, informality and emigration behavior may limit the ability to increase the precision of measuring unemployment, inadequate safety nets and the relatively high level of self-employed persons in the country might contribute to the underestimation of output-unemployment relationship.

Future research may need to focus on alternative approaches to assess the Okun relationship with various model specifications and lag length selections, along with variable transformation such as other ratios of labor market indicators or the "gaps" version. The latter, for instance,

could be invaluable in taking into account possible changes in the "natural" rate of unemployment and potential output growth, as the Albanian economy strives to catch-up with other higher per capita income countries.

References

An, Z., Ghazi, T. & Prieto, N.G. (2017) "Growth and jobs in developing economies: trends and cycles" IMF Working Paper WP/17/257.

Ball, L., Furceri, D., Leigh, D., & Loungani, P. (2019) "Does one law fit all? Cross-country evidence on Okun's law" Open Economies Review 30, 841–874 (2019).

Bartolucci, F., Choudhry, M.T., Marelli, E. & Signorelli, M. (2018) "GDP dynamics and unemployment changes in developed and developing countries" Applied Economics, 50 (31), 3338-3356.

Blinder, Alan S. (1997) "Is there a core of practical macroeconomics that we should all believe?" The American Economic Review, vol. 87, no. 2, 1997, pp. 240-243.

Cazes, S., Verick, S. & Hussami, F.A. (2013) "Why did unemployment respond so differently to the global financial crisis across countries? Insights from Okun's law" IZA Journal of Labor Policy, Springer; Forschungsinstitut zur Zukunft der Arbeit GmbH, vol. 2 (1), pp 1-18, December.

Farole, T., Ferro, E. & Gutierrez, V.M. (2017) "Job creation in the private sector: an exploratory assessment of patterns and determinants at the macro, sector, and firm levels" Jobs Working Paper, no. 5. World Bank, Washington D.C.

Garo, O. (2020) "Inquiring into the relationship between the unemployment rate and output growth", Paper presented at Bank of Albania, 14th South-Eastern European Economic Research Workshop, Tirana, 10-11 December 2020.

IMF (2010) "World Economic Outlook. Chapter 3"

Lee, S., Schmidt-Klau, D., Weiss, J., Chacaltana, J. (2020) "Does economic growth deliver jobs? Revisiting Okun's Law" ILO Working Paper 17, November / 2020.

Okun, A. (1962) "Potential GDP: its measurement and significance" Proceedings of the Business and Economic Statistics Section of the American Statistical Association.

Pizzo, A. (2019) "Literature review of empirical studies on Okun's law in Latin America and the Caribbean" ILO Employment Policy Department Working Paper No. 252, 2019.

Prachowny, M.J.F. (1993) "Okun's law: Theoretical foundations and revised estimates" The Review of Economics and Statistics, vol. 75, no. 2, 1993, pp. 331-336.

Vika, B., Vika, I. (2021) "Forecasting Albanian time series with linear and nonlinear univariate models" Academic Journal of Interdisciplinary Studies, Richtmann Publishing, vol. 10, no. 5, September 2021.

Katalogimi në botim – (CIP)
Biblioteka Kombëtare e Kosovës "Pjetër Bogdani"

004 :658 (496.51) (062)

Proceedings International Conference : proceedings of the 11th UBT Annual International Conference : international Conference on Information Systems / edited by Edmond Hajrizi. - Prishtinë : UBT, 2022. - 47 f. : ilustr. ; 30 cm.

1. Hajrizi, Edmond

ISBN 978-9951-550-85-7

INTERNATIONAL CONFERENCE ON BUSINESS,TECHNOLOGY AND INNOVATION

CHAPTERS:

- Computer Science and Communication Engineering
- Management, Business and Economics
- Mechatronics, System Engineering and Robotics
- Energy Efficiency Engineering
- Information Systems and Security
- Architecture – Spatial Planning
- Civil Engineering, Infrastructure and Environment
- Law
- Political Science
- Journalism, Media and Communication
- Food Science and Technology
- Pharmaceutical and Natural Sciences
- Design
- Psychology
- Education and Development
- Fashion
- Music
- Art and Digital Media
- Dentistry
- Medicine & Nursing

Lagjja Kalabria p.n KS - 10000, Prishtinë
+383 38 541 400
+383 38 542 138

www.ubt-uni.net
conferences@ubt-uni.net

ISBN 978-9951-550-85-7
9 789951 550857