CYBERSECURITY RISK-MANAGEMENT TO MAINTAIN INTEGRITY LAND DATA TRANSACTIONS: APPLICATION TO INDONESIAN AND FRENCH LAND ADMINISTRATION SYSTEMS

P. F. Blin[1], T. Aditya[1], C. Claramunt[2], Y. Kermarrec[3], P. B. Santosa[1]

[1] Universitas Gadjah Mada, Department of Geodetic and Geomatic Engineering, Yogyakarta, Indonesia – pierre.francois.blin@mail.ugm.ac.id, triasaditya@ugm.ac.id, purnamabs@ugm.ac.id

[2] Naval Academy Research Institute, Lanvéoc-Poulmic, France – christophe.claramunt@ecole-navale.fr

[3] Institut Mines-Telecom Atlantique, Departement of Computer Science, Brest, France – yvon.kermarrec@imt-atlantique.fr

KEY WORDS: Cybersecurity Risk-Management, Cadastre, Land Data Transactions, Land Administration System

ABSTRACT:

This paper introduces a series of principles for cyber risk management applied to Land Administration Systems. The aim is to maintain the integrity of cadastral data and land transactions while maintaining vulnerability awareness and risk treatment. The methodology combines BPMN 2.0, EBIOS Risk Manager and Obérisk in compliance with ISO standards. The approach is comparatively applied to Indonesian and French cadastres as a proof-of-concept to foster reproducibility and scalability and provide further opportunities for application to other international Land Administrations Systems.

1. INTRODUCTION

In all countries of the world, a transition from paper to digital availability of land cadastres and registers has accelerated towards more Land digitalisation and IA geo-processing, without users being aware of the cybersecurity of land data (FIAN International, 2020). With the digital convergence of cadastres and land registers, the integrity of land data is essential for maintaining trust among institutions, businesses and citizens, and therefore avoiding being a target for cyber-attacks (Gryszczyńska, 2016; Makala & Anand, 2018). Although land management research and implementations have made significant progress, cybersecurity and cyber risk management are hardly developed. Risk management has been mainly studied for disasters and natural hazards (Yomralioglu & Mclaughlin, 2017). Even in the latest Framework for Effective Land Administration (UNGGIM, 2020), which considers "Land data is the core of Land Administration", the terms cyber and integrity of data are not considered. Similarly, publications of the Office International du Cadastre et du Régime Foncier (OIRCF) and the International Federation of Surveyors (FIG) do not consider the issue.

The objectives and aims of this research are to anticipate the vulnerabilities, threats and risks of a Land Administration System (LAS) and to propose mitigating solutions, by developing a socio-technical methodology of cyber-risk management (Ottens & Stubkjær, 2008). An important aim is to build a reproducible methodology in a cross-disciplinary approach (Falco et al., 2019) that combines geomatics, computer science and risk management principles. The validation and feasibility of our method will be evaluated by applying it to two complementary LAS case studies (i.e., cultural, historical, functional, and organisational) as a Proof-of-Concept for reproducibility and scalability. Cyber attacks will be anticipated and evaluated concerning the integrity of land data transactions and territorial governance. The role of land valuation is an essential basis for land taxation, delimitation and categorisation of buildings, territorial and urban planning, control of land use, and not just a system for securing the land property (Roy & Viau, 2008). In practical terms, the objectives are first to identify similarities and differences between the two considered LAS at each methodological step to promote appropriate and personalised solutions that integrate technical but also cultural and social dimensions. Secondly, each case study will evaluate to which degree the considered LAS is safe and what measures should be implemented to improve its cybersecurity. Third, specific attention will be given to the categories of risks associated with land data (e.g., ownership, thematic, spatial) and which ones are the most targeted and vulnerable to cyber-attacks. Fourth, land use categories (e.g., residential, coastline, mines, forests, customary lands) will be evaluated concerning their vulnerabilities to cyber-attacks.

2. RELATED WORK

Mainly highlighted in the non-academic grey literature (landportal.org, grain.org, IRD.org), the digitisation of land cadastres and registers is currently generating potential conflicts and cyber security threats because "cybersecurity by design" is not part of the land digitisation process. With the massive digitisation of cadastres and the increase in their interoperability (Makala & Anand, 2018), their attack surface has expanded. Such threats might impact government services (Grant et al., 2020), land valuation, land use planning and many LAS services (Astor et al., 2017). Early forerunners who warned about cyber threats to cadastral data and the need to apply security came from Finnish researchers (Riekkinen et al., 2016, Krigsholm et al., 2020). This probably came from the fact that Finland's LAS is well established and reliable (UNGGIM, 2020). These authors mentioned the lack of awareness of security issues and the current lack of expertise in cyber risk management in the LAS, both at decision-makers and operational staff levels. The Kadaster authors revealed a gap in the literature on land administration maintenance, particularly on the importance of securing land rights and transaction information (Bennett et al., 2021) through forgery and fraud (Samsudin, 2020). What clearly appears is that a methodology for managing cyber-risks to maintain the integrity of topological and semantic land data is currently lacking. This entails the need for the development of a generic socio-technical

methodology, applicable to all LAS, and to identify the sources of risks and reasons for threats, quantify their impacts and understand whether existing approaches are satisfactory to address risks as well as residual risks.

3. PROPOSED METHODOLOGY

The research method will be conducted in Indonesia (Jakarta Utara LAS) and France (Finistère LAS) with a comparative analysis using a sequence of deliverables: (1) BPMN (Business Process Modeling Notation), land data integration to evaluate internal and external actors of a given LAS (2) scenario-based socio-technical risk management based on EBIOS risk management, (3) comparative analysis of each of the different risk management steps of the two case studies. Two culturally, historically, functionally and organisationally LASs are considered: the Agraria dan Tata Ruang/Badan Pertanahan Nasional (ATR/BPN) of Jakarta Utara (Indonesia)(Van et al., 2018) and the Délégation Départementale des Finances Publiques du Finistère (SDIF) of Finistère (France). As cyber risk management surely involves anticipation, rather than reaction, to mitigate future cyber threats, and close connection to the underlying LAS spatio-temporal models (Mango et al... 2022), our methodology must be adapted to the needs of each LAS. Moreover, international standards and ISO norms will be considered, as well as scalability and interoperability, using a scenario-based rather than IT-based approach (ENISA, 2022). This should favour a socio-technical approach (Kioskli & Polemi, 2021) adapted to the cultural specificities, different levels of computerisation, human users intervention and third-party partners and stakeholders of each LAS. The chosen methodology is based on internationally approved and standardised methods:

- BPMN 2.0 to identify the LAS data and ownership life cycle,

- EBIOS Risk manager as a method of cyber risk management is the only one referenced by ENISA (ENISA, 2022) for its socio-technical (Asset-based/Scenario-based) and interoperable (Quantitative/Qualitative) approach and recommended by ANSSI (French National Cybersecurity Agency) with its capitalisation of numerous experiences and applications to vast and different domains.

- Obérisk (Paul & al.;2021) to guide semi-structured data collection interviews involving stakeholders in the study of scenarios through EBIOS RM workshops. This provides the right information and affects people in the security process, as many security problems are related to a lack of cyber awareness.

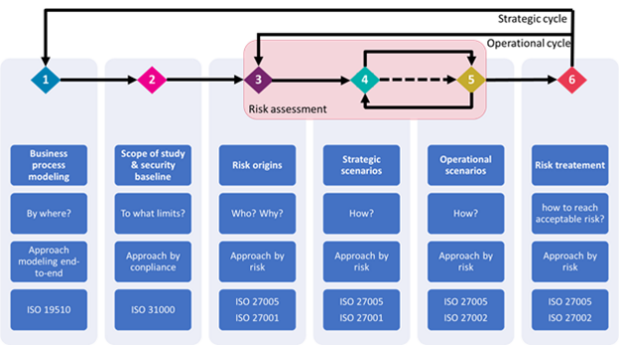

Table 1. Flowchart methodology components

Inspired by BPMN 2.0 and EBIOS RM, the research methodology integrates ISO 19150, 27001, 27002, 27005 and 31000 standards, qualitative (descriptive) and quantitative (measurable) data are collected according to the Obérisk approach (Paul et al., 2021). The six steps methodology (Table 1) will be applied successively to SDIF Finistère and ATR/BPN Jakarta Utara; the collected data will be analysed and compared by divergence or convergence for each step.

Applying this methodology will provide cyber risk management and risk treatment to secure land data transactions of the Jakarta-Utara ATR/BPN and Finistère SDIF, but more importantly, a Proof-of-Concept of the replicability of our methodology.

4. PROOF OF CONCEPT

The two case studies are the ATR/BPN of Kota Administrasi Jakarta Utara (Indonesia) and the SDIF Finistère (France) and are spatially comparable LAS entities. Each one has a coastal maritime territory and undergoes strong urban development (land reclamation and urban sprawl), intense land pressure with very high land prices, and is also subject to the of climate change. These two territories are also respectively their national leaders in cybersecurity: Brittany region is the French national centre for cybersecurity and cyberdefense, and Jakarta is the IT capital of Indonesia. Within those study cases, two territorial sub-entity villages are selected (Kecamatan Penjaringan and the commune of Crozon) as Proof-of-Concept to prove the validity of the chosen methodology and its generic potential. A comparative analysis of the results of the two case studies will be performed to (1) evaluate to which degree our methodology is sufficiently flexible, generic and fit-for-purpose to be generalised and implemented, as illustrated in Table 2, to apply other LAS geodata services perimeters (2 and 3).

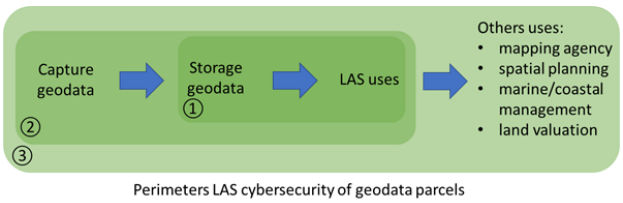

Table 2. LAS geodata services

5. CONCLUSIONS

The research's outcome is to confirm that the design and implementation of a cyber risk management methodology for Land Data Administration provides a structured framework to define, assess and document threats, vulnerabilities, risk sources and impacts. Secondly, we propose a continuous improvement plan for mitigating cyber risks to the integrity of land data transactions. The objective is to provide an agile, integrated, and structured environment for each of the six steps of a cyber risk management process. This should enable future LAS cybersecurity experts to have a high level of control over the production process, identify and manage risks, and improve availability, trust and confidence in land transactions processes and LAS cybersecurity. Moreover, the use of international standards in the development and implementation of this methodology and the harmonisation of deliverables at each stage (a) ensures the interoperability of information between LAS services and partners, (b) provides an environment for applying consistent and objective methods of cybersecurity control, (c) meets the needs of each LAS on the budgetary capacities (human resources, technical resources, and organisational resources). Future research may focus on the following issues: extending to other areas of the LAS (Table 2), extending towards the cyber-risk management of geodata of cadastre 4D and real estate property using digital-twin Building Information Models (BIM).

ACKNOWLEDGEMENTS

This study is derived from Pierre-François Blin's doctoral thesis currently under progress a the Universitas Gadjah Mada.

REFERENCES

Astor, Y., Sulasdi, W. N., Hendriatiningsih, S., & Wisayantono, D. (2017). The Evaluation of Marine Cadastre Definitions Among Australia, Canada and United States of America Based on Indonesia's Perspective as an Archipelagic State. In Cadastre: Geo-Information Innovations in Land Administration (pp. 275–308). Springer.

Bennett, R. M., Unger, E. M., Lemmen, C., & Dijkstra, P. (2021). Land Administration Maintenance: A Review of the Persistent Problem and Emerging Fit-for-Purpose Solutions. Land 2021, Vol. 10, Page 509, 10(5), 509. https://doi.org/10.3390/LAND10050509

ENISA. (2022). INTEROPERABLE EU RISK Methodology for and assessment of interoperability (Issue January). https://doi.org/10.2824/07253

FIAN International. (2020). Disruption or Déjà Vu? Digitalization, Land and Human Rights Mapping of Digitalization and Blockchain Projects in the Land Secto. https://www.fian.org/files/files/FIAN_Research_Paper_Digitalization_and_Land_Governance_final.pdf

Grant, D., Enemark, S., Zevenbergen, J., Mitchell, D., & McCamley, G. (2020). The Cadastral triangular model. Land Use Policy, 97, 104758. https://doi.org/10.1016/J.LANDUSEPOL.2020.104758

Gryszczyńska, A. (2016). Cybersecurity of public registers in Poland: Selected legal issues. GIS ODYSSEY 2016, 105.

Kioskli, K., & Polemi, D. (n.d.). A Socio-Technical Approach to Cyber Risk Assessment. Article in International Journal of Electrical and Computer Engineering. Retrieved April 9, 2022, from https://www.researchgate.net/publication/345673984

Krigsholm, P., Riekkinen, K., & Ståhle, P. (2020). Pathways for a future cadastral system: A socio-technical approach. Land Use Policy, 94, 104504. https://doi.org/10.1016/J.LANDUSEPOL.2020.104504

Makala, B., & Anand, A. (2018). Blockchain and land administration. UNOPS.

Paul, S., & Varela, P. (2019). Poster Support for an Obeya-Like Risk Management Approach. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11720 LNCS, 155–185. https://doi.org/10.1007/978-3-030-36537-0_8

Riekkinen, K., Toivonen, S., Krigsholm, P., Hiironen, J., & Kolis, K. (2016). Future themes in the operational environment of the Finnish cadastral system. Land Use Policy, 57, 702–708. https://doi.org/10.1016/j.landusepol.2016.06.039

Samsudin, S., Zakariah, Y., & Ngadiman, N. (n.d.). An Overview of the Fraud and Forgery Challenges in Land Registration System European Journal of Molecular & Clinical Medicine An Overview of the Fraud and Forgery Challenges in Land Registration System.

UNGGIM. (2020). Framework for Effective Land Administration Expert Group on Land Administration and Management United Nations Committee of Experts on Global Geospatial Information Management (UN-GGIM) Content.

Yomralioglu, T., & Mc Laughlin, J. (2017). Cadastre: Geo-information innovations in land administration. In Cadastre: Geo-Information Innovations in Land Administration. https://doi.org/10.1007/978-3-319-51216-7