Information Security Governance in Distributed Systems Architecture

Ana-Maria Florescu

Information Security Governance in Distributed Systems Architecture

First year PhD Candidate: Florescu Ana-Maria
Aix-Marseille University, CERGAM, FEG
Aix-en-Provence, France
ana-maria.florescu@univ-amu.fr

Supervisor: Vitari Claudio
Aix-Marseille University, CERGAM, FEG
Aix-en-Provence, France
claudio.vitari@univ-amu.fr

Supervisor: Amabile Serge
Aix-Marseille University, CERGAM, FEG
Aix-en-Provence, France
serge.amabile@univ-amu.fr

Abstract: *Given the current challenges surrounding information security, such as social engineering, negligence, poor cyber hygiene, poor data management to configuration mistakes, denial of service, data theft and cybercrime dangers, this research proposal seeks to undertake a comprehensive exploration of information security governance, with a specific focus on distributed systems architecture. The research question of this paper is: How existing information security governance frameworks are applicable to a distributed system architecture, taking into account Elinor Ostrom's principles on governing the commons?*

Keywords: *information security, information security governance, distributed systems*

Introduction

Cybersecurity is one of the critical aspects of today's Information Systems, as the number of cyberattacks is rising daily. The more digital the world becomes, the more technology we use, the more vulnerabilities exist. IS security threats can be found all over, from social engineering, negligence, poor cyber hygiene, poor data management to configuration mistakes (Jang-Jaccard & Nepal, 2014). From natural disasters, such as floods, fires, and earthquakes to malevolent dangers such as denial of service, data theft and cybercrime dangers such as espionage, activism, terrorism, and more (Fantino, 2018, p. 11). Phishing, denial of service and malware are the most cited security vulnerabilities out there (Humayun et al., 2020, p. 13). Cybercrime is always evolving and becoming more and more sophisticated. Threats are becoming more complex and with a larger impact surface.

At the same time, organisations' information systems are even more vulnerable (Humayun et al., 2020, p. 13). The reasons are multiple. From one hand, when it comes to individual level, security culture includes several dimensions: organisation's attitude, awareness, behaviour, competency. On an organisational level, cybersecurity culture includes the following dimensions: assets, continuity, access and trust, operations, defence, security governance (Georgiadou et al., 2022, p. 4). Some obstacles in dealing with threats should be raised as well: increased complexity, lack of awareness, lack of knowledge, lack of incentives, lack of monitoring and enforcement (Harbers et al., 2018, p. 2218).

As a consequence, people are sizing the impact in terms of data and financial loss, repairs costs, legal consequences for non-compliance with existing regulations, reputation damage, and even risks of interruption of service and clients loss (Fantino, 2018, pp. 193–194).

Most of the times, in order to protect themselves, organisations implement different governance and management frameworks, to name a few: NIST cybersecurity framework, the ISO 2700X standard (an international benchmark for information security management system), directives

and intern security policies, as well as methods such as "plan, do, check, act" that helps to define, assess and deal with information security risks and implement security measures (Disterer, 2013).

Cybersecurity is impacting everyone, as it permits infrastructure and businesses to function properly. At the same time, we do live in a very interconnected world, where a cyberattack occurred in the US can affect users from France, Germany or Australia. An attack on an infrastructure system that occurred in eastern Europe can directly affect western Europe organisations, and vice versa. The same reasoning comes to networks, an attack that occurs in one node is capable to impact the entire system.

Nevertheless, days of protecting an easily defined perimeter against most threats are gone. Existing pointed solutions used by most actors cannot respond to complex occurring risks, especially in complex systems, such as distributed ones. There's an increasing need for a continuous process type of solution in order to embrace all permanent challenges.

Conceptual Background

Cybersecurity is defined as "protecting information assets by addressing the threats to information processed, stored and transported by internetworked information systems" (von Solms & von Solms, 2018, p. 5) and as the "preservation of confidentiality, integrity and availability of information in the cyber environment" as defined by the ISO 2700X standard. Cybersecurity is closely related to other security domains, including information security, network security and internet security. For the purpose of simplifying the analysis of this paper, concepts of information security and cybersecurity would be considered as synonyms.

Governance is analysed in terms of processes and mechanisms by which organisations, institutions or societies make and enforce decisions and policies.

IT governance refers to the ways technologies are managed, regulated, directed and the processes by which decisions are made: "how decisions are made, who makes the decisions, who is held accountable, and how the results of decisions are measured and monitored are all parts of IT governance" (Symons, 2005).

IS security governance is defined by the "measures taken to effectively plan, manage, and improve information security" (Georgiadou et al., 2022, p. 3).

Cybersecurity governance is analysed in terms of the mechanism through which an organisation directs and controls security, establishes the accountability framework and offers supervision to ensure that risks are appropriately mitigated, whereas management ensures that policies to minimise risks are executed.

A distributed system is seen in terms of "a collection of distinct processes which are spatially separated, and which communicate with one another by exchanging messages" (Lamport, 1978, p. 558). An example of a distributed system is a "a network of interconnected computers" (Lamport, 1978, p. 558).

In this context, cybersecurity governance in distributed systems presents a challenge, due to their complex nature. Their decentralisation makes it difficult to implement traditional measures that were designed for centralized structures and creates a need for new approaches and frameworks, that consider both technical and organizational aspects. The key element

includes a comprehension of characteristics, as well as threats and risks associated with distributed systems, as well as the integration of cybersecurity into their overall design.

The most known example of distributed system would be the blockchain technology, that is based on a "decentralised framework, utilises peer-to-peer networks and distributed systems" (Hasanova et al., 2019, p. 1). Using blockchain technology means a drop in costs regarding the launching and operating of a digital platform (Catalini, 2018, p. 37).

Blockchain Technology

Blockchain technology uses a peer-to-peer structure, is capable to "provide to communities: tokenization, self-enforcement and formalisation of rules, autonomous automatization, decentralisation of power over the infrastructure, increasing transparency, and codification of trust" (Rozas et al., 2021, p. 1).

From one hand, blockchain is a service like any other that needs to be secured, but on the other hand, blockchain can enhance existing security. Blockchain by itself has some similarities with cybersecurity, a technology that "enables secure transactions and sharing data" (Catalini, 2018, p. 38) and benefits: increased security, transparency, traceability and efficiency.

By using blockchain technology to "decentralise domain name resolution (e.g., Blockstack), computing (e.g., Ethereum), and file storage (e.g., FileCoin, Storj, Sia)", organisations could "improve their resilience to hacks, outages, and bugs" (Catalini, 2018), as a decentralised system is much more difficult to be attacked. Blockchain is also of benefit for digital privacy and data confidentiality, as it "enables the verification of transaction attributes and credentials" (Catalini, 2018, p. 38). Blockchain technology permits to "establish immutable audit trials and data integrity" (Catalini, 2018, p. 39).

Blockchain has "the potential to transform how people and businesses cooperate" (Shackelford & Myers, 2016, p. 382) and organisations are "using blockchain to enhance cybersecurity" as "blockchain allows industries to return to a decentralised Internet, (...) that is safer than centralised" (Shackelford & Myers, 2016, p. 355). It is capable of providing the ability "to control individuals' own personal data" (Kshetri, 2017, p. 10). "When machines become capable of implementing cryptographic security, most of the current hacking activities can be eliminated or at least reduced" (Kshetri, 2017, p. 10).

It is of importance that governing processes and actions related to cybersecurity inside these systems could be made in an efficient manner, with a responsible allocation of resources, a resilient approach and the development of a more sustainable cyber environment.

In this context, the objective of this research is to assess how existing governance frameworks are applicable to a distributed system in order to guarantee its confidentiality, availability, integrity, authenticity and non-repudiation.

It is interesting to analyse and evaluate cybersecurity governance in the context of distributed systems, for example, such as blockchain. By researching the topic of cybersecurity governance in distributed systems, one can gain an understanding of the best practices and strategies for ensuring that these systems are secure and resilient.

The question is: how cybersecurity governance frameworks are applicable to a distributed system?

Distributed Systems

A distributed systems is seen in terms of "a collection of distinct processes which are spatially separated, and which communicate with one another by exchanging messages" (Lamport, 1978, p. 558). An example of a distributed system is a "a network of interconnected computers" (Lamport, 1978, p. 558). Different types of networks are distinguished: centralized, decentralized and distributed, each offering its own advantages and disadvantages (Rehman et al., 2022).

Distributed networks are like decentralized ones in the way that the processing and storage resources are distributed among multiple nodes. However, in a distributed network, nodes work together to complete a task, rather than making independent decisions. The processing is spread evenly across all the nodes. This type of network is highly efficient and secure, as there is no single point of failure. However, it can also be more difficult to manage, as the nodes must communicate and coordinate with each other in order to complete a task.

When it comes to distributed and decentralized systems, the main difference between the two lies in the nature of control and decision-making process. The existence of numerous nodes in distributed systems poses a significant challenge to formulating and implementing effective cybersecurity policies. The lack of a central authority accountable for its security intensifies the challenge. It is critical to establish a precise and well-defined governance framework.

Distributed system is "an information-processing system that contains a number of independent computers that cooperate with one another over a communications network in order to achieve a specific objective" (Puder et al., 2006, p. 8). In other terms, it's "a collection of independent entities that cooperate to solve a problem that cannot be individually solved" (Kshemkalyani & Singhal, 2007, p. 1).

Distributed systems are considered to be "more reliable, and when architected correctly, they can lead to much more scalable organizational models" (Burns, 2018, p. 2).

A distributed system architecture in an inter-organizational context is a system in which multiple organizations or entities work together to achieve a common goal. In this architecture, each organization maintains its own systems and resources, but they are connected and communicate with each other through a network. Distributed systems offer numerous advantages over centralized systems, such as better scalability, reliability and fault-tolerance. They can be more cost-effective, as they can make use of cheaper commodity hardware and can be designed to operate in a more energy-efficient manner.

From the technical perspective, a distributed system architecture is characterized by the fact that "information from each computing unit is shared with the common communication system" and has way more advantages compared to a centralized system architecture, by being more scalable, fault-tolerant, cost-effective and where each individual module or node can be created, tested, and upheld autonomously (Jo et al., 2014, p. 3).

Information Security Governance

Corporate governance, IT governance and Information Security governance are three interconnected concepts that play an essential role in organisations. Solms and Solms (2009) provide a diagram that explains the relationship between them.

In this context, corporate governance refers to “the set of processes, customs, policies, laws and institutions affecting the way a corporation is directed, administered or controlled” (Solms & Solms, 2009, p. 2). The primary objective of which is to ensure an effective management, protect the interests of stakeholders and ensure accountability and transparency. It “relates to the way a company is run and managed in order to ensure its well-being” (Solms & Solms, 2009, p. 1).

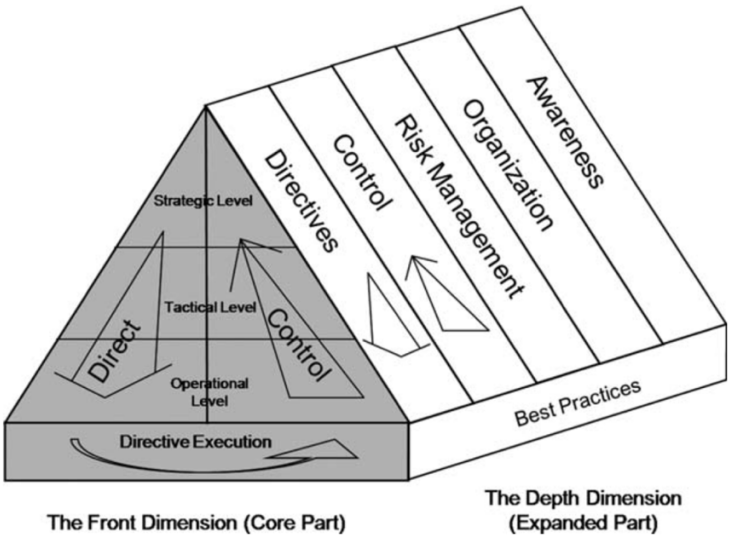
IT governance, on the other hand, is concerned with the procedures that guarantee the alignment of the organization's IT with its strategies and goals and its capacity to uphold and enhance them. IT governance encompasses resource allocation, risk management, performance monitoring, value measurement and stakeholder collaboration to achieve organizational objectives and ensure IT effectiveness.

When it comes to the concept of Information Security Governance, Solms and Solms (2009) describe it as the set of processes that ensures the confidentiality, integrity, and availability of an organization's information assets. ISG represents the collective effort of management commitment and leadership, organizational structures, user awareness, policies, procedures, processes, technologies, and compliance enforcement mechanisms. The aim of Information Security Governance is to ensure the ongoing confidentiality, integrity, and availability of the company's electronic assets, including data, information, software, hardware and personnel (Solms & Solms, 2009, p. 24).

Information Security Governance Framework

One of the proposed Information Security Governance Model (Solms & Solms, 2009) is a comprehensive framework that organizations can use to manage their information security projects. The model is designed to align an organization's information security objectives with its overall business strategy and to ensure that information security risks are managed in a consistent, integrated and cost-effective way.

Information Security Governance Model (Solms & Solms, 2009, p. 31):



Governing the Commons

The concept of a common good in economics is characterized as a type of good that is non-excludable and rivalrous in consumption. This implies that no individual or group can be excluded from using the good, while the consumption of the good by one individual prevents its simultaneous consumption by other individuals. Elinor Ostrom, a Nobel prize-winning political economist, was instrumental in popularizing the term common good. Ostrom described common goods as "long-enduring, self-organized and self-governed" goods (Ostrom, 1990, p. 143). She conducted extensive research into how people can manage shared resources such as forests, fisheries, oil fields, and irrigation systems to resolve the tragedy of the commons.

According to Elinor Ostrom, there are several key factors that ensure the sustainable use of shared resources. These factors include:

1. Clearly defined boundaries are essential to prevent overuse or exploitation of the shared resource.
2. Rules and regulations should be tailored to the specific context of the distributed system and consider the needs and preferences of all stakeholders.
3. Collective-choice arrangements are necessary to ensure that all stakeholders have a say in how the shared resource is managed.
4. Monitoring mechanisms are critical to ensure compliance with rules and regulations.
5. Graduated sanctions can be used to deter non-compliance with rules and regulations.
6. Conflict resolution mechanisms should be in place to address disputes that may arise between users or stakeholders.
7. Minimal recognition of the rights to organize means that users and stakeholders should have the freedom to organize themselves and participate in the governance of the system as they see fit.
8. Nested enterprises are necessary to ensure that the governance of the system is aligned with broader social and economic goals.

Distributed systems architecture can be thought of as a type of commons – a shared resource that needs to be governed and managed effectively. It enables multiple users to access shared resources and services. Resources are distributed across multiple nodes or computers, enabling users to work together as a unified system.

In Elinor Ostrom's framework for governing the commons, common-pool resources such as water, forests, and fisheries are characterized by being a shared resource. This feature is also applicable to distributed system architecture. In a distributed system, the available resources are shared among multiple stakeholders. Therefore, it is essential to govern the use of these resources effectively to ensure their continued availability to all stakeholders.

One of the sub-questions of this research would be: Which Elinor Ostrom's principles of governing the commons can be applied to information security governance in distributed systems?

The analysis could emphasise the importance of clear boundaries, rules for use, and monitoring and enforcement mechanisms in ensuring the security and integrity of data in a distributed system.

Methodology

In order to answer the research question, multiple cases method is proposed. A case study research is "an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin, 2009, p. 18).

Multiple cases study will help "to understand the similarities and differences between the cases and therefore provide the literature with important influences from its differences and similarities" (J. Gustafsson, 2017).

The criteria for case selection are based on relevance, representativeness, uniqueness and data availability (Small, 2009).

References:

Burns, B. (2018). *Designing Distributed Systems: Patterns and Paradigms for Scalable, Reliable Services*. O'Reilly Media, Inc.

Catalini, C. (2018). Blockchain Technology and Cryptocurrencies: Implications for the Digital Economy, Cybersecurity, and Government. *Georgetown Journal of International Affairs*, *19*, 36–42.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*, 92–100. https://doi.org/10.4236/jis.2013.42011

Fantino, B. (2018). *Quels élements d'influence pour l'adoption symbolique de la sécurité des systèmes d'information?* [These de doctorat, Aix-Marseille]. https://www.theses.fr/2018AIXM0586

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, *62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Harbers, M., Bargh, M., Pool, R., Van Berkel, J., Van den Braak, S., & Choenni, S. (2018). *A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges*. http://hdl.handle.net/10125/50166

Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M.-S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), e2060. https://doi.org/10.1002/nem.2060

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jo, K., Kim, J., Kim, D., Jang, C., & Sunwoo, M. (2014). Development of Autonomous Car—Part I: Distributed System Architecture and Development Process. *IEEE Transactions on Industrial Electronics*, *61*(12), 7131–7140. https://doi.org/10.1109/TIE.2014.2321342

Kshemkalyani, A. D., & Singhal, M. (2007). *DISTRIBUTED COMPUTING: PRINCIPLES, ALGORITHMS, and SYSTEMS.*

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. In *TELECOMMUNICATIONS POLICY* (Vol. 41, Issues 10, SI, pp. 1027–1038). ELSEVIER SCI LTD. https://doi.org/10.1016/j.telpol.2017.09.003

Lamport, L. (1978). *Time, clocks, and the ordering of events in a distributed system*. *21*(7).

Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press.

Puder, A., Römer, K., & Pilhofer, F. (2006). *Distributed Systems Architecture: A Middleware Approach*. Elsevier.

Rehman, A. U., Aguiar, R. L., & Barraca, J. P. (2022). Fault-Tolerance in the Scope of Cloud Computing. *IEEE Access*, *10*, 63422–63441. https://doi.org/10.1109/ACCESS.2022.3182211

Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2021). When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance. *SAGE Open*, *11*(1), 21582440211002526. https://doi.org/10.1177/21582440211002526

Shackelford, S., & Myers, S. (2016). Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2874090

Small, M. L. (2009). `How many cases do I need?': On science and the logic of case selection in field-based research. *Ethnography*, *10*(1), 5–38. https://doi.org/10.1177/1466138108099586

Solms, S. H., & Solms, R. (2009). *Information Security Governance*. Springer US. https://doi.org/10.1007/978-0-387-79984-1

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Yin, R. K. (2009). *Case Study Research: Design and Methods*. SAGE.