From Observing to Understanding: Empirical Insights on the Organizational Foundations of Security Chaos Engineering

Short Paper

Jacqueline Strobel
FIM Research Center for Information Management, University of Bayreuth
Bayreuth, Germany
jacqueline.strobel@fim-rc.de

Florian Weiß
FIM Research Center for Information Management, Branch Business & Information Systems Engineering of the Fraunhofer FIT
Bayreuth, Germany
florian.weiss@fim-rc.de

Michael Bitzer
FIM Research Center for Information Management, Augsburg University of Applied Sciences, Branch Business & Information Systems Engineering of the Fraunhofer FIT
Augsburg, Germany
michael.bitzer@fim-rc.de

Abstract

Cloud computing has become an integral part of modern corporate IT infrastructures. However, conventional IT-security measures cannot cope with its specific technical needs resulting from complexity, virtualization, or multi-tenancy as well as the need for holistic security approaches incorporating both technological and organizational perspectives on security. Security Chaos Engineering (SCE) constitutes a promising approach to overcome these shortcomings. Unfortunately, existing literature focuses on technical aspects of SCE and neglects the organizational perspective, i.e., which organizational success factors need to be addressed for a successful implementation. To close this gap, we conducted an interview study following the approach of Gioia et al. (2013) and identified seven success factors related to goals, social structure, participants, and technology within a company following Scott (1981). *Furthermore, we found that these organizational success factors are not only the basis for the introduction of SCE but represent common requirements for holistic security approaches in general, too.*

Keywords: Cloud Security, Security Chaos Engineering, Interview Study

Introduction

Cloud computing has become a crucial part of today's digital value creation across most sectors due to its on-demand self-service and pay-per-use logic, as well as broad network access (NIST 2011). In 2021, around 90% of companies already used cloud computing systems (Flexera 2021). However, the growing usage of cloud computing also raises IT security concerns (PwC 2022), especially since more than 85% of companies embrace a multi-cloud concept which even increases complexity (Flexera 2023). While larger cloud providers can ensure high security levels for individual cloud services (Demissie and Ranise 2021), the combination and integration of different cloud services in certain businesses can lead to unforeseen

consequences for the overall cloud security, e.g., creating vulnerabilities for intentional attacks or accidental system failures (Halton and Rahman 2012). Accordingly, cloud misconfigurations were the number one reason for security incidents in 2022 (Schulze 2022). Consequently, security is one of the top three concerns of all types of organizations regarding cloud computing, with more than 70% being highly concerned about cloud security (Flexera 2023). Due to the complexity of cloud architectures resulting from especially the heterogeneity of cloud environments, i.e., the multitude of configuration options of both single and multi-cloud systems (Flexera 2023) together with a missing holistic perspective including technical as well as organizational aspects (Torkura et al. 2021), traditional security approaches cannot cope with resulting challenges (Gritzalis et al. 2021; Torkura et al. 2020). Thus, practitioners and researchers have expressed the need for novel security approaches to resolve this issue (Parast et al. 2022).

Security Chaos Engineering (SCE), an evolution of Netflix´s Chaos Engineering (CE) approach (Rinehart and Shortridge 2020), is discussed by practitioners and academia as a suitable approach to addressing the issues resulting from complex cloud security requirements (Rinehart and Shortridge 2020; Torkura et al. 2020). In contrast to traditional security approaches, SCE is a holistic approach, including both technical tooling and organizational measures (Rinehart and Shortridge 2020). SCE strives to allow for comprehensive understandings of complex systems by examining the effects of unexpected changes and by preventing undesired effects proactively (Lewis and Wang 2019; Sharieh and Ferworn 2021). To achieve this goal, SCE includes the implementation of automated experiments within respective cloud environments to intentionally cause security-relevant events in production or production-like environments aiming for vulnerability discovery and resolving underlying issues before they lead to actual incidents (Rinehart and Shortridge 2020). Until today, existing literature regarding SCE is mostly limited to technical recommendations and examples. Some papers provide exemplary experiments and corresponding configurations (e.g., Lewis and Wang 2019; Torkura et al. 2019), while others discuss the architecture of potential SCE tooling (e.g., Rinehart and Shortridge 2020; Torkura et al. 2020). Some researchers also discuss artifacts used within SCE such as decision trees or prioritization matrixes (e.g., Podjarny 2020; Rinehart and Shortridge 2020). However, even though Rinehart and Shortridge (2020) portray the first small use cases for SCE and first relevant organizational considerations such as the underlying culture or events to be integrated, it does not become clear what is mandatory for a successful implementation of SCE. Against this backdrop, we address the following research question:

Which fundamental success factors are relevant for the implementation of SCE?

To answer our research question, we conducted an in-depth interview study (Schultze and Avital 2011). For data analysis, we relied on the systematic approach by Gioia et al. (2013). In the interviews with IT security experts, we cover the implementation process of SCE, including required steps, processes, and resources, as well as the general security mindsets prevalent in companies together with the corresponding objectives. From our preliminary analysis, we identified seven success factors (SF) for an implementation. The SF can be grouped into goals, social structures, participants, and technology as suggested by the framework of Scott (1981), and match the current cloud security transformation happening in companies. Our research contributes to theory by structuredly examining challenges and objectives in the context of cloud security and the consequences for security solutions. Further, we combine IS research with organizational research demonstrating the relevance of organizational considerations in the context of IT security. Regarding practice, we identified fundamental SF that are essential for a successful implementation of SCE as representative of holistic security approaches including e.g., hacking events or security responsibles in development teams. In the following, we present the current literature regarding cloud security and SCE, our research design, our preliminary results, a short discussion, and the expected contribution of our work.

Theoretical Foundations

Cloud Security as a Major Challenge for Cloud Computing

Until today, cloud computing has gained significant attention for its cost-efficient as well as high-quality services and has enabled companies to outsource IT infrastructure operations to both enhance their services and increase their value (Parast et al. 2022). It refers to "ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [...] that can be rapidly provisioned and released with minimal management effort" (NIST 2011). Novel characteristics, such as virtualization, high levels of on-demand scalability, and multi-tenancy provide the basis for the realization of large synergies (NIST 2011).

However, the resulting heterogeneity of cloud environments, i.e., the multitude of design options for architectures, services, and deployment models, drive complexity and, thereby, increase the attack surface as well as the number of potential sources of error compared to isolated on-premises data centers (Lewis and Wang 2019). Accordingly, practitioners have deployed reactive security measures such as incident response measures or preventive procedures such as threat analyses and penetration testing, as well as the implementation of standards like ISO 27001 (Simić-Draws et al. 2013). However, due to the complexity and dynamic nature of cloud environments, practitioners require approaches to addressing security continuously and proactively to avoid intentional or unintentional system failures resulting in service interruptions or losses of both trust and reputation (Lewis and Wang 2019; Torkura et al. 2019).

Further, research agrees that it is important to consider systems within companies from both a technical and organizational perspective as sociotechnical systems to increase acceptability and value add for stakeholders (Baxter and Sommerville 2011). Also in the context of security, it is essential to consider both technical and organizational aspects (Viganò 2022). Until today, conventional security approaches cannot sufficiently address these requirements, making novel holistic approaches or an extension of existing approaches imperative (Gritzalis et al. 2021; Torkura et al. 2021). One recently discussed promising approach addressing this gap is SCE (Podjarny 2020; Shortridge and Rinehart 2023). Therefore, we examine SCE as an approach, representative for the class of those incorporating an integrated view of both organizational and technical dimensions, with the potential to fill the identified gap in research.

Security Chaos Engineering as Security Solution for Cloud Computing

SCE is a novel approach that is discussed by practitioners and academia as a possible solution to building and manifesting a proactive corporate security culture, which is derived from the principles of Chaos Engineering (CE) focusing on cloud availability (Torkura et al. 2020). A fundamental assumption of the CE paradigm is that vulnerabilities are almost impossible to avoid in dynamic and complex environments like cloud architectures (Sharieh and Ferworn 2021), which is why CE strives to create fault-tolerant systems by automatically, continuously, and proactively introducing errors into running systems (Rosenthal and Jones 2020). This way, CE allows cloud operators to continuously learn how their systems behave under varying conditions and to detect failures before they cause unintended downtimes for customers (Basiri et al. 2016).

However, the CE approach exclusively addresses availability issues and neglects further security-relevant properties such as integrity and confidentiality, whose adherence is crucial for cloud operation, too (Basiri et al. 2016). Since there is no such thing as total security, especially distributed cloud systems should not only be designed securely but fault-tolerant and easy to restore, i.e., resilient, as well (Nino and Chaves 2021; Rinehart and Shortridge 2020). As CE has proven to be an adequate approach to address those aspects in the context of availability, the concepts and principles of CE have been expanded to a more complete security approach called Security Chaos Engineering (SCE) addressing availability, integrity, and confidentiality (Rinehart and Shortridge 2020). SCE is defined as a "discipline of instrumentation, identification, and remediation of failure within security controls through proactive experimentation to build confidence in the system's ability to defend against malicious conditions" (Rinehart and Shortridge 2020) and "address the challenge of security incidents resulting from human errors and misconfigured resources" (Torkura et al. 2019). It is an integrative approach including not only technical resources such as experimentation software but also a novel security mindset including principles such as "failure is normal", as well as further organizational aspects including an extensive feedback culture and close cross-functional collaboration for integrating SCE successfully (Rinehart and Shortridge 2020). In the end, the introduction of SCE should create a culture where people aim to understand and improve their software in a continuous process instead of expecting perfect artifacts right away as well as creating confidence among (security) teams regarding their systems and abilities to deal with (unforeseen) failures (Lewis and Wang 2019; Sharieh and Ferworn 2021).

Unfortunately, even though SCE is a holistic approach, the available literature on SCE is mainly limited to technical recommendations, e.g., detailed descriptions of potential experiments, necessary codes, attack graphs, and attack points (Rinehart and Shortridge 2020; Torkura et al. 2020). The organizational lens, however, including necessary resources or processes, potential challenges occurring, or preparation necessities are mainly neglected except for general considerations such as integrating a learning and feedback culture (Rinehart and Shortridge 2020). To close this gap in research, this paper investigates on the SF that must be taken into consideration for successfully implementing SCE.

Preliminary Research Design

Research Method

Since our study sheds light on a novel phenomenon, we follow an exploratory approach and conduct an in-depth interview study as a proven method for data collection in qualitative research (Schultze and Avital 2011). For data analysis, we relied on the systematic approach by Gioia et al. (2013), which, in academia, has been used to create novel theories with scientific rigor focusing on semi-structured interviews for data collection (Gioia et al. 2013). During the process of data collection, the guideline and sometimes even the initially identified research question need to be revised to match evolving insights (Gioia et al. 2013). The data analysis consists of three steps. First, *first order concepts* are created by coding interviews using informant-based terms to capture all relevant information which results in a vast number of initial codes (Gioia et al. 2013). Second, researchers start analyzing first order concepts for similarities and differences and group concepts into categories leading to *second order themes* reducing the number of unstructured codes (Gioia et al. 2013). This step helps to further develop the interview guideline and select additional interview partners based on the already acquired knowledge (Gioia et al. 2013). In the third step, the second order themes are distilled even further into *aggregate dimensions* (Gioia et al. 2013). Finally, this data structure is used as the basis for an *inductive model* showing the relationships among the emergent concepts clarifying the connection between data and developed theory (Gioia et al. 2013).

Data Collection

To understand the logic of SCE, we conducted an initial unstructured literature review regarding both CE and SCE. Additionally, to understand existing challenges for the adoption of SCE in an organizational context, we conducted three 60 minutes interviews with both CEOs of a consulting start-up working on cloud security solutions and a doctoral candidate, who has already published multiple contributions in the context of SCE and focused on SCE and the development of a corresponding tool within his research.

Based on the initial interviews, we concluded that a lot of organizations are currently in the process of a cloud security transformation but are still likely to lack both the required mindset and structures to adopt SCE effectively. We also determined the target group of SCE in a workshop together with one of the CEOs of the cloud security start-up discussing relevant company characteristics together with SCE requirements. Finally, we identified three main types of organizations that should consider SCE: Organizations with (1) a strong digitalization background, (2) underlying regulatory requirements facing stricter rules regarding IT security, and (3) a sufficient budget for adequate IT security. Within these organizations, SCE is important for all employees dealing with software development in the cloud context and managers responsible for the organization's IT security. Based on these insights together with the literature analysis, we developed an initial interview guideline and started to reach out to potential interview partners ranging from technical implementers to budget managers to gain a holistic understanding incorporating all relevant perspectives.

In total, we have conducted 17 interviews with 18 different interview partners from various business fields including IT services, consulting, or banking, and different professional backgrounds such as CISOs, security architects, or heads of IT security. Beforehand, we provided the interview guideline as well as a short presentation introducing SCE as most interviewees did not know SCE before the interview. All interviews took between 45 and 60 minutes and were both conducted and recorded via Microsoft Teams. To ensure completeness and avoid biases, two researchers participated in most of the interviews. Within the first five interviews, we applied our initially developed interview guideline discussing three main topics: (1) the status quo of cloud security in companies, (2) the feasibility of a SCE implementation in a company, and (3) a fictive implementation of SCE including topics such as required steps, processes, or resources as well as expected challenges before or during the implementation. After five interviews, we conducted a coding workshop discussing which topics to continue and which additional interview partners had to be recruited in consequence. Based on the workshop, we found that the security mindset and its perception within companies constitute major challenges for an effective implementation of SCE and, thus, should be a focus of the next interviews. Therefore, we adapted our interview guideline and recruited C-level executives as further interview partners to dive deeper into this topic.

Data Analysis

During the data analysis, we strictly followed the approach suggested by Gioia et al. (2013). After transcribing the interview recordings, we coded the interview transcripts according to the interview guideline's structure using the open coding function of MAXQDA. After the first three interviews, all researchers conducted another coding workshop to guarantee a mutual understanding of the data and coding structure. With ongoing coding and developing of the coding structure, regular workshops among all authors have been conducted to accompany the coding process. Within this process, we extracted a total number of 1,350 text excerpts and 288 first order concepts. During the third step, we included memos summarizing critical aspects and brainstorming potential relationships and concepts helping to understand the correlation between the identified concepts and building second order themes. As this process is iterative, we switched between clustering first order concepts into second order themes and refining them based on novel insights. This process involved weekly coding workshops among all authors in which they discussed the clustering process, the clusters themselves, as well as the results' interpretations. This coding step resulted in 17 second order themes. In the fourth step, we again clustered the second order concepts into four aggregate dimensions. Table 1 gives an overview of the identified second order themes together with the aggregate dimensions. During the analysis, we identified major similarities of our interviews with organizational theory addressing relevant areas in companies, especially in the context of change. Thus, we decided to structure our findings in accordance with the organizational model provided by Scott (1981) as it is a well-established framework in scientific research with more than 17,000 citations and has already been applied multiple times in IS literature (e.g., Jonathan et al. 2020; Lavassani and Movahedi 2017). Our results are structured along the proposed framework as presented in the subsequent section.

Second order themes	Aggregate dimensions
Status quo: minimum effort security	Goals
Goal: security integral in companies, products	
Status quo normative structure: legal compliance and missing anchoring of security in companies	Social Structure
Goal normative structure: organization-specific guidelines and security as an important part of the big picture	
Status quo behavioral structure: separated, late-stage tasks and missing collaboration	
Goal behavioral structure: support for secure development and cross-functional, cross-hierarchical collaboration	
Management: from missing interest to interest in implementing security	Participants
Security team: from separated security teams to security people integrated into projects	
Employees: from missing interest to interest in implementing security and perception of security as value add	
Customers: from missing interest to interest in implementing security	
Status quo security measures: late stage, separated architectonic, internal, external, incident response measures	Technology
Goal security measures: holistic, integrated security measures	
Status quo security processes: security integrated separated, late stage in development processes	
Goal security processes: security holistically integrated into development processes	

Table 1: Coding Results based on Gioia et al. (2013)

Preliminary Results

As explained in the previous sections, the need for an integrated approach to ensuring cloud security arises from changing requirements that existing solutions cannot cope with. Among other approaches incorporating both organizational and technological dimensions, SCE is one solution that can be implemented to ensure corporate cloud security. However, to be able to successfully implement SCE, it is crucial that several fundamental requirements are met. Preparing the determination of SF for a SCE implementation, we first identified and structured critical changes regarding cloud security on the basis of the framework by Scott (1981) focusing on goals, social structure, participants, and technology as key organizational areas. In this regard, *goals* mean the conditions participants want to affect with their activities. *Social Structure* defines the relationships among participants including the formats and channels for collaboration. *Participants* are the individuals contributing to companies incorporating individual characteristics like their mindsets, ambitions, and capabilities. *Technology* refers to mechanisms creating a company's outputs. In addition to the traditional understanding of single technologies, the design and implementation of processes are considered here. Figure presents the transition from the respective status quo of the past to today's requirements of all these aspects. Afterwards, we elaborate on these transitions in more detail as well as their implications for a SCE implementation resulting in seven SF.

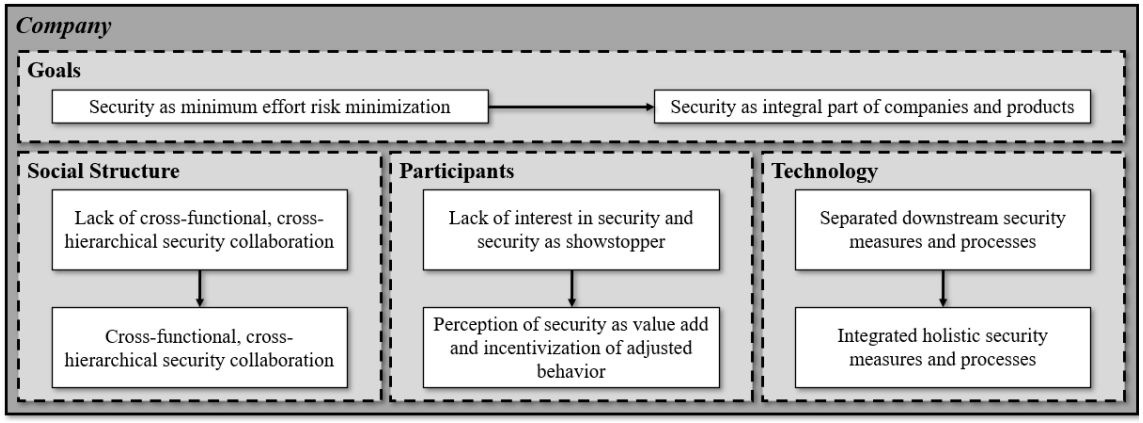

Figure 1: The Evolution of (Cloud) Security Requirements based on Scott (1981)

Goals

Regarding Goals, our interview partners consistently reported that a lot of companies only conduct security measures with rather minimal effort to reduce the most threatening risks and ensure compliance with regulations and most important customer expectations.

The objective that companies should follow is to integrate security as a critical functional requirement and value add compared to other companies. *"So, when I studied, it was still like that, yes, security is a non-functional property. I just think that since we have all systems hooked up to the net in some way, […] since then, it's not a non-functional property, it's a functional property."*

SF1: Cloud security is a crucial functional requirement. This should also be reflected on both the strategy and operation levels.

Social Structure

The status quo of the Social Structure in companies is characterized by a lack of cross-functional and cross-hierarchical collaboration regarding security. The main reasons are missing structures regarding security for development and the integration of security personnel into the process only at the end of the development cycle. *"As soon as you have the opportunity to report, which must be read and officially taken note of in writing, then they must act accordingly."* In addition, incentive systems were reported to be at least partially conflicting with security ambitions (little dedicated capacities and bonuses depending on "number of completed lines of code" instead of "number of secure lines of code".

Thus, the objective is to anchor security practices in the company through adequate structures and integrate security people during the whole development process as a supporting function. *"These are the people who help me in this thicket, in this jungle of some kind of regulations that exist from outside […]. Well, then it's good for a team if they know there's someone to help me through this jungle. "*

SF2: In addition to sufficient resource allocations (both time and budget), incentive systems that support instead of conflict with the achievement of security goals should be ensured, to not only provide the means but also incentivize security benefitting behavior.

SF3: A successful implementation of SCE requires a goal-oriented rather than a problem/responsibility-oriented form of collaboration. Assuming that everyone is doing their best, even when mistakes occur, teams should work together to find solutions rather than looking for who is to blame.

SF4: Implement hacking events to strengthen collaboration. Introduce as many stakeholders as useful to security issues and foster their motivation by demonstrating how cloud security issues can be resolved through collaboration.

Participants

Today, a lot of participants show a lack of interest in security as they perceive security mostly as showstoppers within development processes. Usually, security teams are separated from other teams, if there are dedicated security teams at all, and sometimes even negative sentiments were reported to exist regarding them. *"These are the people who kind of come around the corner and then sort of stand up and intervene when the system is built. And that's frustrating for a development team."*

The goal is to create motivation among all relevant stakeholders based on the valuation of security. Also, security experts or responsibles should be integrated into development and operation teams to encourage security adequate behavior. *"We have the vision that at some point in every team you have at least one security champion, who takes the issue particularly seriously, who then also motivates his colleagues*."

SF5: Find and encourage security ambassadors in all teams (voluntariness and intrinsic motivation strongly increase the effectiveness) and convene rounds for regular exchange e.g., on best practices between them.

Technology

Technology includes security measures commonly applied in current times which are mainly about checking for compliance and are adopted at the end of the development cycle without proper integration into regular processes from early stages on.

Our interviews found that the goal in this regard is to implement more holistic security measures such as internal in-depth testing from the beginning of the development cycle or conducting early-stage vulnerability experiments. Regarding security processes, companies were reported to aspire to more standardized and automized solutions to effectively integrate security into the early phases of regular processes. *"The sooner we test dynamically and really have tools that help us to understand the software or to test the software and then generate vulnerability reports, the cheaper and the better it is."*

SF6: Develop experiments that are both automized and scalable to a maximum extent.

SF7: Consider useful experiments as early as the conceptual design stage, conduct, and refine experiments while the development process is still underway so that potential errors can be noticed and corrected early. The development process of experiments alone can already lead to insights.

Discussion

Even though this work focuses on SCE, SCE is only exemplary for a whole group of holistic approaches covering the technical together with the organizational perspective. Other approaches are, for example, resilience engineering which helps to increase the resilience of socio-technical systems by quantifying technical and social resilience dimensions such as risk management process steps or (technical) resilience capabilities of stakeholders (Häring et al. 2016). All these holistic approaches will face the same organizational challenges when being considered for an implementation meaning that the identified results, i.e., the SF, are not only relevant for an SCE integration but for the whole group of (holistic) approaches.

Considering the choice of interview partners, we tried to reach out to people who have already gained experience with explicitly implementing SCE into their own company. However, there are hardly any companies that have already implemented this concept making it difficult to identify practical SCE experts. Thus, we decided to speak with general IT professionals whereas some of them have already gained experience with implementing the similar approach of CE. Consequently, the identified SF should be considered as fundamental requirements paving the way for a successful implementation of SCE without the claim of completeness. In order to provide a more complete and practically tested SF, additional interviews with SCE experts that have already implemented SCE or according case studies are necessary. Also, such studies will be required to evaluate how far the fundamental SF presented are sufficient or need to be further developed e.g., providing more details about the actual implementation process.

Expected Contribution

With our work, we expect to extend the existing body of knowledge with both theoretical and practical contributions. Our first theoretical contribution involves examining how the requirements for cloud security solutions have evolved over time, based on the framework of Scott (1981). Secondly, we identified important success factors from the perspective of practitioners. Although most of these SF are already described in a similar or even analogous way in SCE literature (e.g., Rinehart and Shortridge (2020), we pinpointed and confirmed the most crucial ones from a practitioner perspective. The practical contribution of this work involves the examination of the identified SF in the form of actionable recommendations. This supports practitioners in determining how far their companies meet the most fundamental requirements of SCE and provides actionable recommendations on how to close potentially existing gaps.

Outlook

We plan to accomplish further steps toward our final goal. First, we plan to conduct further coding sessions as well as additional interviews to review both our developed model presented in Figure 1 and SF to validate or further evolve them with cloud security experts. Second, during the interviews, we examined that the current cloud security transformation of companies does not only raise the necessity to adopt SCE or a similar approach, but that such implementations can also support companies during their transformation, too. Thus, we additionally plan to explore these mutual effects more in detail.

References

Basiri, A., Behnam, N., Rooij, R. de, Hochstein, L., Kosewski, L., Reynolds, J., and Rosenthal, C. 2016. "Chaos Engineering," *IEEE Software* (33:3), pp. 35-41 (doi: 10.1109/MS.2016.60).

Baxter, G., and Sommerville, I. 2011. "Socio-Technical Systems: From Design Methods to Systems Engineering," *Interacting with Computers* (23:1), pp. 4-17 (doi: 10.1016/j.intcom.2010.07.003).

Demissie, B. F., and Ranise, S. 2021. "Assessing the Effectiveness of the Shared Responsibility Model for Cloud Databases: the Case of Google's Firebase," in *2021 IEEE International Conference on Smart Data Services*, N. Atukorala (ed.), Chicago, IL, USA. 9/5/2021 - 9/10/2021, Piscataway, NJ: IEEE, pp. 121-131 (doi: 10.1109/SMDS53860.2021.00026).

Flexera (ed.). 2021. "2021 State of the Cloud Report: COVID-19 Accelerates Cloud Plans and Spend as More Organizations Adopt Multi-Cloud Strategies," Flexera.

Flexera (ed.). 2023. "2023 State of the Cloud Report: Economic Volatility Doesn't Slow Cloud Growth; FinOps Increases in Priority," AWS and Azure Continue to Battle for Dominance, Flexera.

Gioia, D. A., Corley, K. G., and Hamilton, A. L. 2013. "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organizational Research Methods* (16:1), pp. 15-31 (doi: 10.1177/1094428112452151).

Gritzalis, D., Stergiopoulos, G., Vasilellis, E., and Anagnostopoulou, A. 2021. "Readiness Exercises: Are Risk Assessment Methodologies Ready for the Cloud?" in *Advances in Core Computer Science-Based Technologies*: *Papers in Honor of Professor Nikolaos Alexandris*, G. A. Tsihrintzis (ed.), Cham: Springer International Publishing AG, pp. 109-128 (doi: 10.1007/978-3-030-41196-1_6).

Halton, W. M., and Rahman, S. 2012. "The Top Ten Cloud-Security Practices in Next-Generation Networking," *International Journal of Communication Networks and Distributed Systems* (8:1/2), pp. 70-84 (doi: 10.1504/IJCNDS.2012.044323).

Häring, I., Ebenhöch, S., and Stolz, A. 2016. "Quantifying Resilience for Resilience Engineering of Socio Technical Systems," *European Journal for Security Research* (1:1), pp. 21-58 (doi: 10.1007/s41125-015-0001-x).

Jonathan, G. M., Rusu, L., and Perjons, E. 2020. "Organisational Structure's Influence on IT Alignment: The Case of a Public Organisation," in *Information Systems*: *16th European, Mediterranean, and Middle Eastern Conference, EMCIS 2019, Proceedings*, M. Themistocleous and M. Papadaki (eds.), Dubai, United Arab Emirates. 09.12.2020-10.12.2020, Springer, Cham, pp. 471-485 (doi: 10.1007/978-3-030-44322-1_35).

Lavassani, K. M., and Movahedi, B. 2017. "Applications Driven Information Systems," *International Journal of Innovation in the Digital Economy* (8:1), pp. 61-75 (doi: 10.4018/IJIDE.2017010104).

Lewis, J., and Wang, C. 2019. "Chaos Engineering: New Approaches to Security," Rain Capital.

Nino, Y., and Chaves, J. G. 2021. *Securing the Cloud*, online.

NIST. 2011. *The NIST Definition of Cloud Computing*: *Recommendations of the National Institute of Standards and Technology*, Gaithersburg, MD, USA: NIST (NIST Special Publication (SP) 800-145) (doi: 10.6028/NIST.SP.800-145).

Parast, F. K., Sindhav, C., Nikam, S., Izadi, H. Y., Kent, K. B., and Hakak, S. 2022. "Cloud Computing Security: A Survey of Service-Based Models," *Computers & Security* (114), pp. 1-18 (doi: 10.1016/j.cose.2021.102580).

Podjarny, G. 2020. *Security Chaos Engineering - What It Is and Why Should You Care?*: *With Aaron Rinehart from Verica*. Podcast.

PwC (ed.). 2022. "A C-Suite United on Cyber-Ready Futures: Findings from the 2023 Gobal Digital Trust Insights," PwC.

Rinehart, A., and Shortridge, K. 2020. *Security Chaos Engineering*: *Gaining Confidence in Resilience and Safety at Speed and Scale*, Sebastopol, CA, USA: O'Reilly Media.

Rosenthal, C., and Jones, N. 2020. *Chaos Engineering*: *System Resiliency in Practice*, Beijing, Boston, Farnham, Sebastopol, Tokyo: O'Reilly.

Schultze, U., and Avital, M. 2011. "Designing Interviews to Generate Rich Data for Information Systems Research," *Information and Organization* (21:1), pp. 1-16 (doi: 10.1016/j.infoandorg.2010.11.001).

Schulze, H. 2022. "2022 Cloud Security Report," Check Point and Cybersecurity Insiders (eds.), Check Point, Cybersecurity Insiders.

Scott, W. R. 1981. *Organizations: Rational, Natural, and Open Systems*, Englewood Cliffs, NJ, USA: Prentice-Hall.

Sharieh, S., and Ferworn, A. 2021. "Securing APIs and Chaos Engineering," in *2021 IEEE Conference on Communications and Network Security (CNS),* Tempe, AZ, USA. 04.10.2021 - 06.10.2021, IEEE, pp. 290-294 (doi: 10.1109/CNS53000.2021.9705049).

Shortridge, K., and Rinehart, A. 2023. *Security Chaos Engineering*: *Sustaining Resilience in Software and Systems*, Beijing, Boston, Farnham, Sebastopol, Tokyo: O'Reilly.

Simić-Draws, D., Neumann, S., Kahlert, A., Richter, P., Grimm, R., Volkamer, M., and Roßnagel, A. 2013. "Holistic and Law Compatible IT Security Evaluation: Integration of Common Criteria, ISO 27001/IT-Grundschutz and KORA," *International Journal of Information Security and Privacy* (7:3), pp. 16-35 (doi: 10.4018/jisp.2013070102).

Torkura, K. A., Sukmana, M. I., Cheng, F., and Meinel, C. 2019. "Security Chaos Engineering for Cloud Services: Work In Progress," in *18th International Symposium on Network Computing and Applications*, A. Gkoulalas-Divanis and D. R. Avresky (eds.), Cambridge, MA, USA. 9/26/2019 - 9/28/2019, Piscataway, NJ: IEEE, pp. 1-3 (doi: 10.1109/NCA.2019.8935046).

Torkura, K. A., Sukmana, M. I., Cheng, F., and Meinel, C. 2020. "CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure," *IEEE Access* (8), pp. 123044-123060 (doi: 10.1109/ACCESS.2020.3007338).

Torkura, K. A., Sukmana, M. I., Cheng, F., and Meinel, C. 2021. "Continuous Auditing & Threat Detection in Multi-Cloud Infrastructure," *Computers & Security* (102), pp. 1-18 (doi: 10.36227/techrxiv.13108313.v1).

Viganò, L. 2022. "Formal Methods for Socio-Technical Security," in *Coordination Models and Languages*: *24th IFIP WG 6.1 International Conference, COORDINATION 2022, Proceedings*, M. H. ter Beek and M. Sirjani (eds.), Lucca, Italy. 13.06.2022-17.06.2022, Cham: Springer International Publishing; Imprint Springer, pp. 3-14 (doi: 10.1007/978-3-031-08143-9_1).