sciendo

Scientific Bulletin
Vol. XXVIII, No. 1(55), 2023

THE PHYSIOGNOMY OF MODERN MULTINATIONAL OPERATIONS

Andra-Ioana PÎNZARIU
andra.pinzariu21@gmail.com

"NICOLAE BĂLCESCU" LAND FORCES ACADEMY, SIBIU, ROMANIA

ABSTRACT:

In this article we intend to analyze the change in the physiognomy of modern military actions starting from the idea that it is extremely important to present the necessary clarifications on the content and meaning of the phrase physiognomy and, just as importantly, to position this concept in direct relation with the most important characteristics of the contemporary military phenomenon, the evolution tendencies of the military art, its levels and, last but not least, its content. Also a derivative objective would be to highlight the bad role of technology and technology in the changes produced in the last period of time in this field.

KEYWORDS:

Multinational operations, security environment, military theatres of operations, military art, joint operations

1. Introduction

Organizations of all types are capitalizing on the advantages of cloud computing, such as (a) simplified information technology management, (b) increased remote accessibility, (c) reduced operation costs, (d) manageability, (e) scalability, and (f) availability (Tabrizchi, & Rafsanjani, 2020). The essence of cloud computing consists of distributing personal computing capacity to servers or cloud servers (Jangjou & Sohrabi, 2022). The National Institute of Standards and Technology classifies cloud computing as a business or service model for facilitating convenience, resource sharing, pervasive, and persistent access (Simmon, 2018), delivered through software-as-a-service (SAAS), infrastructure-as-a-service (IAAS), or platform-as-a-service (PAAS) (Tabrizchi & Rafsanjani, 2020). Businesses and organizations seek to capitalize on cloud computing for economic and operational capacity advantages. Resource sharing coupled with scalability and availability are attractive business determinants for leveraging cloud computing.

Cloud misconfiguration errors are problematic in today's hyperactive cybersecurity threat landscape. Technology and security decision-makers list cloud misconfigurations as a severe data security risk caused by human errors impeding security compliance and countering digital transformation initiatives (Coker, 2020). One principal security analyst claims to observe over 230 million misconfigurations daily (Coker, 2020). The COVID-19 pandemic intensified cloud misconfigurations (Paganini, 2021) as organizations raced to

DOI: 102478/bsaft-2023-0010

transition from centralized operational constructs to decentralized operations. Business organizations capitalized on the flexible cloud models, availability, and resource sharing to support work from home. As cloud computing operations increased, so did the misconfiguration errors.

This article highlights using the human factors analysis and classification system (HFACS) to prevent misconfiguration errors in cloud computing. This research serves to instigate discourse and concerns to support the use of HFACS to prevent human errors in cloud computing. Existing literature suggests that human errors and complacency result in misconfiguration errors and data breaches. The HFACS is extensively used in other sociotechnical domains to underpin contributing factors that cause errors and mistakes.

2. Background

In 2017, a reputable security vendor reported that cloud misconfiguration increased by 424 %, resulting in negative implications to the technology ecosystem (Forrest, 2018). Cloud computing dates back to the 1960s, and researchers and practitioners still struggle with integrating human factors (ergonomics) into the cloud environment (Gohary, Hussin, & Razak, 2013). Existing literature notes that cloud computing increases collaboration, expandability, agility, availability, flexibility based on work demands and requirements, and the benefit of cost reduction through optimization and efficient computing (Al-Anzi, Yadav, & Soni, 2014). Although cloud computing provides organizations with tailored computing capabilities, there is a dark side; this growing phenomenon is cloud misconfigurations resulting from human errors. A reputable technological and research firm reported that 95 % of data breaches result from human errors (Rundle, 2019). It is imperative to explore methodologies to reduce cloud misconfigurations, given that existing computing ecosystems are growing increasingly complex and hyperconnected.

3. Cloud computing

According to the National Institute of Standards and Technology: cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (this last part of the definition bear a strong resemblance to usability measures) (Mell & Grance, 2015, p. 8).

Cloud computing consists of the following five characteristics (Branado, 2019; Mell & Grance, 2015): (a) on-demand self-service, (b) broadband network access, (c) resource pooling, (d) rapid elasticity, and (e) measured service. Organizations have the option of choosing from three deployment models: (a) public cloud, (b) private cloud, and (c) hybrid cloud (Kalluri & Rao, 2014). Organizations use IAAS, PAAS, or SAAS service models for cloud computing, as depicted in Figure no. 1, to provide employees with computing solutions based on the five characteristics listed above.

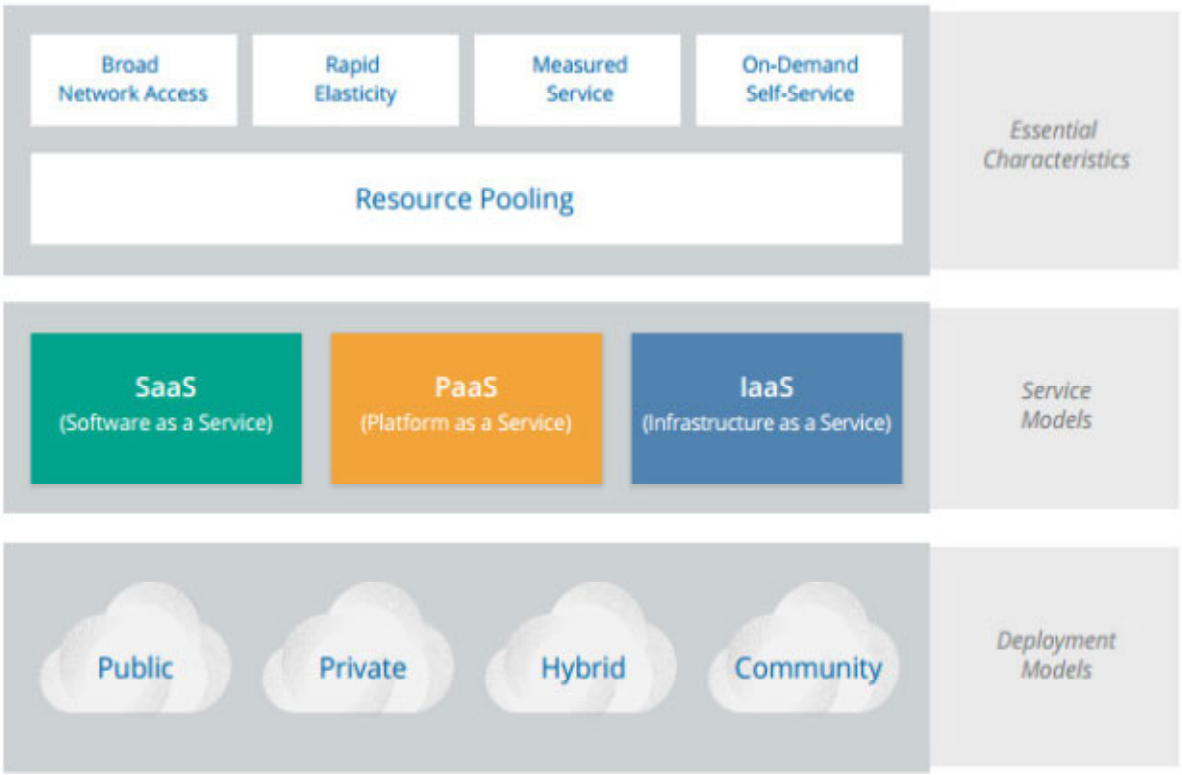

Figure no. 1: NIST Cloud Computing Model
(Source: Courtesy of CSA, 2017)

A unique aspect of cloud computing is the ability of users to access computing resources from anywhere through an internet-connected system (Brandao, 2019). Another optimistic viewpoint of cloud computing is that the user only pays for what is needed, preventing wasting resources, accompanied by scalability, enabling the user to demand additional resources when required (Brandao, 2019). The flexibility of cloud computing allows the transfer of risk or forgo purchasing physical resources and ownership of the contracted infrastructure (Brandao, 2019). Cloud computing as a business model offers organizations a more affordable approach than traditional information technology practices.

While the adoption of cloud computing continues to increase; however, there are significant concerns regarding the cloud. First, misconfiguration errors plague organizations as these blunders could quickly and often result in data breaches (Al-Anzi, Yadav & Soni, 2014; Forrest, 2018; Rundle, 2019). Second, security in cloud computing is of the utmost importance and requires constant upkeep to safeguard against emerging and persistent cybersecurity threats. Third, privacy is a significant issue partially due to organizations transitioning from traditional information technology infrastructure to cloud computing, given that public clouds are target-rich environments for malicious exploitation (Brandao, 2019). Security and privacy are challenging aspects of cloud computing and require better interoperability and tenancy principles to lessen the probability of cyber-attacks. Fourth, data management is complex in the cloud environment because organizations have less control of their data, and multi-tenancy could result in unauthorized access to the data.

4. Misconfiguration errors in cloud computing

A recent report highlights that 75 % of mid-size and large companies will have migrated to cloud computing (Express Computers, 2020). Misconfiguration errors remain a top cloud security concern (Express Computers, 2020). It is essential to highlight that misconfiguration errors in cloud computing are human errors. According to Linthicum (2018), misconfiguration pertains to the public cloud instances, such as compute and storage, which are erroneously designed, increasing the vulnerability to data breaches. For example, a federal entity misconfigured its Amazon S3 instance, enabling accessing secure documents through a browser (Linthicum, 2018).

A universal misconfiguration error leaves unencrypted data stores exposed to the internet without an authentication solution, enabling data to be accessible to all platform users while exposing encryption keys and credentials in the unsecured warehouses (Cook, 2020). The mounting number of misconfigurations indicates talent management issues, resulting in the inability to protect complex hybrid and multi-cloud deployments (Cook, 2020). Paganini (2021) acknowledged human errors as the leading cause of cloud misconfiguration. Poor understanding of cloud security and policies, insufficient controls and oversight, overburden with application programming interfaces, and insider threat incidents contribute to misconfiguration errors (Paganini, 2021).

The 2021 Cloud Misconfiguration Report emphasized that internet-facing misconfigurations have occurred since the onset of the Advanced Research Projects Agency Network, an experimental computer network, the predecessor of the internet (Rapid 7 Research, 2021). The ascendancy of cloud computing resulted in significant miscalculations and misconfiguration errors even as primitive turnkey services were hardened; in today's modern cloud environments, misconfiguration errors frequently occur (Rapid 7 Research, 2021).

Human error contributes to misconfigurations; the belief that software components have safety defaults accompanied by intentional actions to create easier access is a significant causal linkage for data breaches (Rapid 7 Research, 2021). Implementing easier access practices is common knowledge by malicious actors (Rapid 7 Research, 2021); hence, the increasing number of data breaches stemming from misconfiguration errors. In 2020, publicly reported data indicated ten misconfiguration errors a month, resulting in data breaches (Rapid 7 Research, 2021).

A senior cybersecurity executive indicated that cloud misconfiguration errors were not only due to complexity; another factor leading to the errors is subcontracting to third parties and laziness (Rundle, 2019). Deploying systems and infrastructure rapidly in the cloud environment often result in cloud misconfigurations (Rundle, 2019). The cybersecurity domain needs a comprehensive framework for identifying causal factors that result in misconfiguration errors.

5. Human factors analysis and classification system

The lack of scholarly and empirical research on using HFACS to explore misconfiguration errors in cloud computing is at issue. Human mistakes in cybersecurity are complex; Tang et al. (2022) acknowledged that many models, frameworks, and observations reduce human errors in practice; yet, error taxonomies are uncommon in cybersecurity. According to Tang et al. (2022), the HFACS model was designed and initially used to investigate human errors in the aviation sector and subsequently extensively used in different domains. Shappell and Wiegmann (2000), the developers of HFACS, indicated that investigators and analysts struggle to determine the best approach for identifying

and mitigating the contributing factors' sequence of order, specifically those associated with human error.

Without a doubt, the HFACS is adaptable, enabling its application to different situations and industries (Tang et al., 2022). Human factors practitioners and cybersecurity professionals can manipulate HFACS to serve as a framework for preventing and investigating security incidents such as misconfiguration errors in cloud computing.

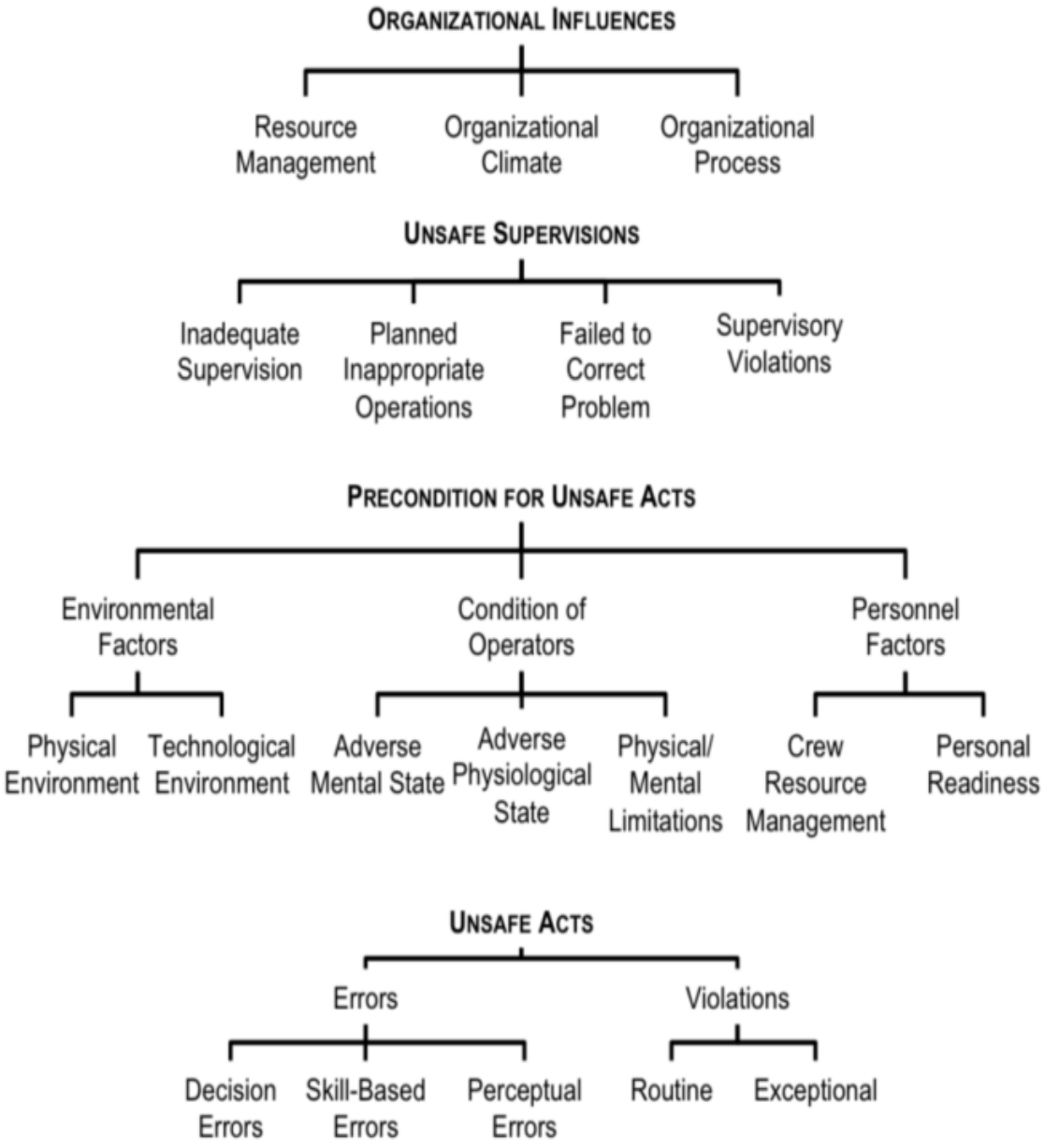

Figure no. 2: The HFACS Model
(Source: Courtesy of https://goflightmedicine.com/human-factors-analysis/hfacs-tree/)

The HFACS model includes the four layers (Organizational Influences, Unsafe Supervision, Preconditions for Unsafe Acts, and Unsafe Acts) originating from the Swiss Cheese Model, as depicted in Figure no. 2. A critical step in leveraging HFACS in exploring misconfiguration errors in cloud computing is the development of nanocodes. The creation of HFACS nanocodes is necessary for cybersecurity and cloud computing to increase the applicability of HFACS in investigating and preventing misconfiguration errors in the cloud, which are human errors.

According to Cohen et al. (2015), the HFACS model leverages nanocodes to classify the contributing factors of an incident/accident. The nanocodes characterize the principal causal category observed in a specific domain (Cohen et al., 2015). In other words, before leveraging HFACS, cybersecurity practitioners would need to develop nanocodes for the subcategories of the four primary categories. For example, using Organizational Processes, a potential nanocode is OP1 (Process Uncodified), OP2 (Process Impractical), or OP3 (Outdated Process). Each subcategory requires a corresponding list of nanocodes.

5.1. Leveraging HFACS to explore misconfiguration errors

It is important to note that cloud misconfigurations are human errors. Therefore, the primary objective of employing the HFACS is to investigate misconfiguration errors in the cloud to prevent future missteps and data breaches. While the HFACS model is predominantly an accident investigation analysis tool (Tang et al., 2022), its applicability could prevent future misconfiguration errors by proactively and consistently exploring potential vulnerabilities within the cloud.

According to Bickley and Torgler (2021), the HFACS framework consists of causal groups of human errors usually applied for logical retrospective incident analysis in high-risk industries. For example, cybersecurity and specifically cloud computing is a high-risk area. The HFACS framework was designed to provide a systematic approach for examining latent and active failures of human-involved activities to identify contributing pathways in which the failures proliferate to incidents. Organizations can reduce cloud misconfigurations errors by using HFACS to aggressively, correctly, and target high-friction areas in cloud computing, notably resulting in misconfiguration errors (Bickley & Torgler, 2021). Even though HFACS analysis occurs after significant incidents, organizations could leverage the HFACS analytical processes to continuously enable cloud engineers and human factors practitioners to highlight weaknesses that could lead to misconfiguration errors.

Leveraging the HFACS in cloud computing is advantageous in providing a proven and systematic approach to incident analysis, such as misconfiguration errors. Existing literature indicates that HFACS applicability and utility to many industries enable reduced investigative process subjectivity and analyses (Bickley & Torgler, 2021; Hale et al., 2012; Reinach & Viale, 2006). While HFACS is ubiquitous in many sociotechnical fields, its use in cybersecurity remains impeded. Given the complexity of cloud computing environments and misconfigurations errors, the HFACS can provide comprehensive insights into the causal factors of misconfiguration errors, thus, affording organizations to implement mitigative and preventative procedures.

6. The benefits of using HFACS

The intersection between technology and security is expanding at an accelerated rate and challenging traditional risk management practices. Cybersecurity is a multidiscipline domain and requires innovative practices to reduce human-based risk. Bickley and Torgler (2021) acknowledge that HFACS is useful in proactive management and prediction of incidents through investigating underlying

pathway analysis. In Figure no. 2, one can observe James Reason's Swiss Cheese Model, particularly leveraging the four hierarchical levels (Bickley & Torgler, 2021). In cloud computing, practitioners can explore the linkages of the hierarchical levels and decision-making at each level that influences and enable the misconfigurations.

Additionally, as depicted in Figure no. 2, the HFACS provides classifications for errors and mistakes, an uncommon practice in cybersecurity. The HFACS will force the classification of errors, mistakes, and violations and assist with determining the causal pathway of misconfiguration errors. Shappell and Wiegmann (2000) postulate that the HFACS brings theory to practices through a comprehensive tool for investigating incidents by focusing on the operators' conditions and organizational influences. In the case of cloud computing, HFACS is a tested framework for identifying the failures and the capability to predict future misconfiguration causal pathways.

7. Conclusions

Misconfiguration errors continue to plague organizations as many businesses transition to cloud environments. Cloud computing is attractive from a cost aspect; however, cloud misconfiguration errors are concerning, especially as hackers and cybercriminals exploit these errors for data breaches. Cloud computing complexity leads to misconfiguration errors. While the existing literature on cloud misconfiguration errors continues to increase, a current gap is the lack of a framework or model highlighting the operators' conditions and how organizations contribute to causal pathways for misconfigurations. The HFACS framework could provide the cybersecurity domain with a tool to effectively prevent and predict future misconfigurations errors in cloud computing. Human errors in cybersecurity are rampant, and HFACS could provide comprehensive analyses from an organizational level to highlight how errors, mistakes, and violations propagate misconfiguration errors – a current blind spot in cloud computing.

REFERENCES

Al-Anzi, F.S., Yadav, S.K., & Soni, J. (2014, September). Cloud computing: Security model comprising governance, risk management and compliance. *International Conference on Data Mining and Intelligent Computing (ICDMIC)*, 1-6, IEEE.

Bickley, S.J., & Torgler, B. (2021). A systematic approach to public health – Novel application of the human factors analysis and classification system to public health and COVID-19. *Safety Science*, *Vol. 140*, 105312.

Brandao, P.R. (2019). Cloud computing security. *IJCST*, *Vol. 10, Issue 1*.

Cloud Security Alliance (CSA). (2017). *Security guidance: For critical areas of focus in cloud computing v4.0*. Available at: https://cloudsecurityalliance.org/guidance/#_overview

Cohen, T.N., Wiegmann, D.A., & Shappell, S.A. (2015). Evaluating the reliability of the human factors analysis and classification system. *Aerospace Medicine and Human Performance*, *Vol. 86, Issue 8*, 728-735, available at: https://doi.org/10.3357/AMHP.4218.2015

Coker, J. (2020, July 23). *Cloud misconfiguration a major compliance risk, say IT decision-makers*. Available at: https://www.infosecurity-magazine.com/news/cloud-misconfigurations-compliance/

dos Santos, V.A., Manacero, A., Lobato, R.S., Spolon, R., & Cavenaghi, M.A. (2020, June). A systematic review of fault tolerance solutions for communication errors in open source cloud computing. *15th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

Express Computer. (2020, April 9). *Misconfiguration is the number one risk to cloud environments, finds Trend Micro Research*. Express Computer. Available at: https://advance-lexis-com.ezproxy1.lib.asu.edu/api/document?collection=news&id=urn:contentItem:5YMD-MMR1-JB5M-W3YX-00000-00&context=1516831.

Forrest, C. (2018, April 4). *Human error led to 424 % increase in misconfigured cloud servers, prompting hacks*. Available at: https://www.techrepublic.com/article/human-error-led-to-424-increase-in-misconfigured-cloud-servers-prompting-hacks/

Gohary, M.M., Hussin, C., & Razak, A. (2013). Human factors' impact leveraging cloud-based applications adoption. *Journal of Information Systems Research and Innovation (JISRI), Vol. 5*, 87-97.

Hale, A., Walker, D., Walters, N., & Bolt, H. (2012). Developing the understanding of underlying causes of construction fatal accidents. *Safety Science, Vol. 50, Issue 1*, 2020-2027.

Jangjou, M., & Sohrabi, M.K. (2022). A Comprehensive Survey on Security Challenges in different network layers in cloud computing. *Archives of Computational Methods in Engineering*, 1-22.

Kalluri, R.K., & Rao, C.G. (2014). Addressing the security, privacy and trust challenges of cloud computing. *International Journal of Computer Science and Information Technologies, Vol. 5, Issue 5*, 6094-6609.

Linthicum, D. (2018). *Cloud misconfiguration: The security threat too often overlooked*. Available at: http://login.ezproxy1.lib.asu.edu/login?url=https://www-proquest-com.ezproxy1.lib.asu.edu/trade-journals/cloud-misconfiguration-security-threat-too-often/docview/2116530107/se-2?accountid=4485

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing (Special Publication 800-145)*. Gaithersburg MD: National Institute of Standards and Technology.

Paganini, P. (2021, April 28). *Cloud misconfiguration, a major risk for cloud security*. Available at: https://securityaffairs.co/wordpress/117305/security/cloud-misconfiguration-risks.html

Rapid 7 Research. (2021, September). *2021 Cloud Misconfigurations Report*. Available at: https://www.rapid7.com/info/2021-cloud-misconfigurations-research-report/

Reinach, S., & Viale, A. (2006). Application of a human error framework to conduct train accident/incident investigations. *Accident Analysis & Prevention*, *Vol. 38, Issue 2*, 396-406.

Rundle, J. (2019, August 27). *Human error often the culprit in cloud data breaches*. Available at: https://www.wsj.com/articles/human-error-often-the-culprit-in-cloud-data-breaches-11566898203

Shappell, S.A., & Wiegmann, D.A. (2000). *The Human Factors Analysis and Classification System – HFACS*. Available at: https://commons.erau.edu/publication/737

Simmon, E. (2018). Evaluation of cloud computing services based on NIST SP 800-145. *NIST Special Publication, Vol. 500*, 322.

Stella, J. (2021). *How to secure cloud infrastructure across the development lifecycle*. Available at: http://login.ezproxy1.lib.asu.edu/login?url=https://www-proquest-com.ezproxy1.lib.asu.edu/trade-journals/how-secure-cloud-infrastructure-across/docview/2577216022/se-2?accountid=4485

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing, Vol. 76, Issue 12*, 9493-9532.

Tang, N., Hu, H., Xu, F., Yeoh, J.K.W., Chua, D.K.H., & Hu, Z. (2022). A personalized Human Factors Analysis and Classification System (HFACS) for construction safety management based on context-aware technology. *Enterprise Information Systems, Vol. 16, Issue 1*, 141-166.