Mathematics and Computer Science
2024, Vol. 9, No. 5, pp. 88-95
https://doi.org/10.11648/j.mcs.20240905.11

Research Article

Managing Security Risks of Public Cloud Computing

Ayokunmi Ogundapo*, Vitus Nnamdi Ezeaputa

Cybersecurity and Human Factor, Bournemouth University, Dorset, England

Abstract

The economic benefits and scalability of public cloud computing are already undeniable due to recent advancements in the field; the only question that remains is cloud security. Despite the enormous benefits of moving their computing workload to the cloud, many organizations continue to show resistance to this change. Cloud security concerns are the most frequently mentioned cause. Organizations are concerned by a larger attack surface created by the worldwide accessibility of services in the cloud. The security and risk control set that enterprises can apply in the cloud is also often limited and impacted by the interoperability and support provided by the chosen Cloud Service Providers (CSPs), and organizations are often not allowed to extend their trusted security solutions they are already familiar with to the cloud. Yet, both traditional computing and cloud computing include security risks, and cloud risk is just as controllable as traditional IT risk. Secondary data obtained from Identity Theft Resource Centre (ITRC) database on cloud incidents from year 2020 to 2022 were analyzed in this study. To determine the primary underlying causes of cybersecurity events observed across the years covered by the available data, the study used trend analysis and descriptive statistics. The analysis shows that cloud incidents are not different from traditional incident and organizations can leverage existing capabilities already developed in traditional computing towards managing the cloud risk. Also, organizations need to take be proactive in their responsibility and take ownership of the risks. As the study shows, the majority of cloud incidents are caused by knowledge gaps and the cloud customer's inability to exercise due diligence and care in ensuring effective controls are put in place to stop prevalent attacks. Effective cloud training and adherence to the established cloud control matrix, like the CSA, would successfully lower risk to a reasonable level.

Keywords

Public, Cloud, Risk, Security, Governance

1. Introduction

Opportunities and risk are brought forth by the development of cloud computing as a constantly changing technology. Many organizations for the economic gains of cloud computing have adopted the cloud in their strategy while many more are considering the cloud as the first model of choice. With the recent advances in cloud computing and improvement recorded in recent years, the economic gains and scalability of cloud computing are no longer in doubt.

Cloud computing refers to the delivery of computing services over the internet. While there is no consensus definition for the term cloud computing, a sizeable number of stakeholders have adopted the National Institute of Standards and Technology (NIST) definition [1]. NIST defined cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, appli-

*Corresponding author: ayokunmi_o@yahoo.com (Ayokunmi Ogundapo)

Received: 16 July 2024; **Accepted:** 17 October 2024; **Published:** 18 November 2024

cations, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. Organizations' access to a ubiquitous, convenient, and shared pool of configurable computing resources means that organizations can escape huge upfront costs associated with traditional computing resources need for business workloads. Cloud computing services are offered on a pay-as-you-use subscription basis thereby enabling organizations the flexibility to manage IT costs by either scaling up or down their computing service consumption relative to the business reality. Despite the enormous benefits cloud computing offers, many businesses and organizations remain reluctant in fully adopting cloud computing because of security risks and privacy concerns of cloud adoption [3].

High-level cyberattacks are now more likely due to the growing popularity of cloud computing and the availability of cloud services via the internet [4]. As IT services move from restricted on-premises perimeters to the cloud, their global accessibility creates a greater attack surface. Even though cloud adoption increases the attack surface, the security and risk control set that organizations can implement in the cloud is frequently constrained and influenced by the interoperability and support offered by the selected Cloud Service Providers (CSPs).

Also, in contrast to traditional computing, where businesses and organizations have firm complete control over the risk landscape and are fully responsible for risk management, cloud computing introduces a shared responsibility model, wherein businesses must share risk with CSPs and trust CSPs to be proactive in addressing cloud computing risk concerns.

With the Original Equipment Manufacturers (OEMs) and software vendors now announcing strategic focus on cloud computing and end of support for historic enterprise applications [5], businesses and organizations are being forced to the cloud and it is imperative for organizations to understand the risk associated with cloud computing in the lens of recent incidents and how to stay afloat while harnessing cloud computing benefits.

2. Background and Challenges

Despite the advantages of cloud computing, many organizations are still behind in tapping into its potential and increasing their competitive edge. Security risk is listed as the top concern of the cloud computing [6]**.** The security risk of cloud computing is the most cited reason for organizations' reluctance to transform the business computing model from traditional computing to the cloud. The fact that cloud security and risk issues are perceived differently between the CSPs and cloud service users is further widening the gaps and reinforcing the concerns [7].

Since businesses also do not own the underlying cloud infrastructures, compliance with jurisdictional standards, regulations, and control may be very difficult in the cloud. This is because service providers having many clients may not see compliance requirements from certain regions as important. For instance, many of the cloud CSPs are already compliant with the European General Data Protection Regulation (GDPR), while only a few are compliant with the Nigerian Data Protection Regulation (NDPR). The bias of CSPs paying more attention to the security and regulatory requirement of their immediate market at the expense of their distant customers is also limiting the options and thus the adoption of the cloud service.

Lack of total control of the computing stack housing sensitive business process information and data also concerns many. The fear is that data entrusted to CSPs may be at risk because the compliance of the cloud service provider to certain standards is difficult to gauge and ascertain. For instance, besides the external threat actors, a rogue employee of CSPs may engage in mining and exploitation of cloud subscribers' data or selling it to competitors and other interested buyers thereby putting cloud-consumer businesses at disadvantage.

The unending breach reports of organizations specialized in IT security solutions, and CSPs continue to create panic for risk-averse organizations, and make others question the safety of their data in the cloud and the sufficiency of the controls in place to mitigate security risks and threats in the cloud.

The security risk and privacy concerns of the cloud are enormous and these need to be brought sufficiently under control to gain general acceptance and wider adoption by businesses. This study, therefore, sought to explore the cloud security trends in the last three years in light of the available control matrix for the cloud incidents observed over the time range.

Traditional Computing Issues

Traditional computing requires every organization to buy the hardware and software required to run their IT operations, and to employ specialized IT personnel to manage different aspects of the IT operations and services. This approach implies that capital expenditure on IT services and operations, which in most cases are secondary to the operation of the business, must be borne upfront. The huge upfront cost of traditional computing served as a drawback for many organizations that needed to raise seed funds to start operations. This can also be regarded as an opportunity cost for large businesses and enterprises whose investments that could otherwise be channeled to other lucrative businesses are tied down in the huge capital cost of IT. If business prospects do not go as projected, the investment made in IT towards such business is rarely recovered.

Growth-minded organizations are further plagued by the purchase of computing capacity for future growth. The extra computing capacity is seldomly used and may sit untapped for the useful life of the computing hardware

Virtualization technology was introduced to reduce cost, drive environmentally sustainable computing and mitigate some of the issues associated with the traditional computing [8]. The primary goal of virtualization is to manage workloads by transforming traditional computing to make it more scal-

able, efficient, and cost-effective [9]. Virtualization makes it possible for organizations to optimize IT costs through the effective use and sharing of computing hardware resources e.g., random memory access (RAM), storage, processor, etc. Virtualizations reduce hardware cost, improves computing data center footprints, and savings on energy bills.

While virtualization serves some useful purposes, it introduces the need for specialized skills to manage the virtualization system itself adding to IT overhead counts and budget. The total cost of ownership (TCO) of virtualization technology is also huge and out of the reach of most SMEs who should benefit from the technology. It also failed to effectively address the need of SMEs who do not want to complicate their business model by managing their IT stack but are satisfied to rent the infrastructure from a willing private cloud provider. The opportunities and lapses in virtualization gave rise to the emergence of cloud computing.

Cloud Computing and Service Models

Cloud computing when compared to traditional IT is quite versatile, more scalable, and more elastic. Cloud computing offers much more benefits when compared to traditional computing [10]. The benefits of cloud computing include the following

i. Pay only for the service used
ii. Resource sharing/pooling among businesses
iii. The main focus is business drive and agility
iv. Service accessibility over the internet
v. Enhanced security beyond what individual businesses can provide themselves
vi. On-demand access to resources
vii. Self-service

Cloud computing offers flexible service models allowing organizations to adopt the model(s) that best suits their requirements. The security concerns in the cloud are reflections of the service models adopted with some degree of responsibility sharing between the consumers and the CSP.

Software as a Service (SaaS): In this model, the cloud consumer uses the cloud provider's application running on the provider's cloud infrastructure. The applications are accessible from various client devices and applications using the internet. The provider is responsible for the administration and control of the underlying cloud infrastructure including host, storage, network, servers, operating systems, and in most cases the application. The application is owned and maintained majorly by the provider, and also has the responsibility for vulnerability closure and threat concern mitigation. The cloud user only owned the data and data protection is however a joint responsibility.

Platform as a Service (PaaS): In this model, the consumer in addition to the shared responsibility of data security is responsible for an application used. The provider provides for underlying cloud infrastructure including host, storage, network, servers, and operating systems but not the application. The consumer owns and is responsible for managing the application and data, and their supporting services. Bug release fixtures and upgrades are more of the worries of the consumer.

Infrastructure as a Service (IaaS): In this model, the capability provided is such that the consumer can provision operating software and applications, install and run arbitrary software and at the same time able to reserve compute resources. The cloud provider still maintains control of underlying cloud infrastructure, but the consumer has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

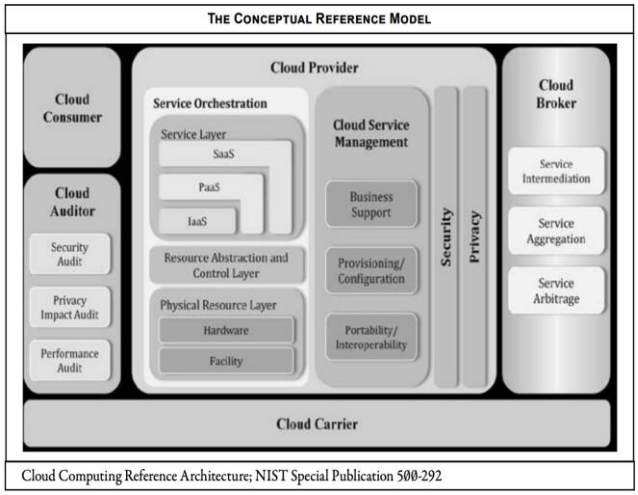

Figure 1. *Cloud Conceptual Reference Model.*

The cloud computing model adopted or subscribed may have a huge impact on the kind of exposure an organization transiting to the cloud may be exposed to, who owns the risk, and who has responsibility for managing and treating the risk. Recent security incident trend in the cloud has shown that cloud security incidents cannot be solely pinned on CSP or consumer. There are incidents resulting from control breakdown and unintentional misconfiguration on the part of the CSPs exposing cloud consumers to risk. Ineffective control implementation on the part of the consumers may also lead to a breach. Recently, Microsoft disclosed [11] a misconfiguration that exposed consumers' data. About 65,000 organizations across 111 countries were affected by the breach [12]. Evidently, cloud breaches may not be because of control breakdown or ineffective cloud governance on the part of the cloud consumers, it can be from either the cloud provider and/or the consumer. It is therefore pertinent to ensure providers are covered in every organization's strategy aimed at cloud adoption or sustenance of service workload in the public cloud.

3. The Risk Mitigation Strategy for Public Cloud Adoption

Yanpei [7] concluded in his research on cloud computing

that security inevitably would become a significant cloud computing business differentiator and that developing security architecture early in the process can pay off greatly. Cloud Security Alliance (CSA), the industry group that provides security guidelines and education for cloud security in its publication [13] states that "security controls for the cloud computing are, for, in most part, no different than the security controls in any IT environment". Organizations with experience in traditional IT therefore already has some experience required to navigate cloud security challenges. However, cloud computing may introduce some different risks to an organization than traditional computing. It is therefore necessary to look at the risk areas of cloud computing and attempt to bring the risks to an acceptable level while the organization continues to benefit from the numerous gains of the cloud.

CSA have further developed a comprehensive and widely accepted cloud security framework to help organizations with a presence in the cloud or transition into the cloud manage their risk and exposures. The CSA framework is comprehensive and involved participation of leading CSPs in its development. The rest of this section considers the guidance set forth by CSA framework. The framework includes the following.

3.1. Governance and Enterprise Risk Management

Governance and Enterprise Risk Management elaborates on the adoption of already established governance frameworks like ISO 38500:2015, ISO 27014:2013, COBIT, etc. Information security is a tool of information risk management, which is a tool of enterprise risk management, which is a tool of governance. The four are all closely related but require individual focus, processes, and tools.

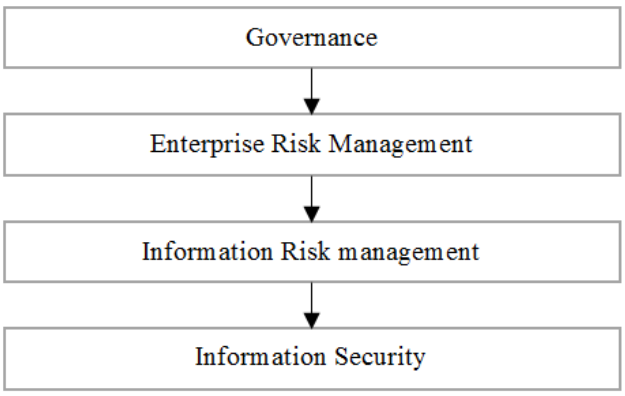

Figure 2. *Governance and Enterprise Framework Cascade.*

Cloud computing affects governance and since information security is a tool of Risk management it cannot be wholesomely taken care of unless it is brought under governance and driven by it. The strength of cloud computing in information risk management is in the ability to manage risk more effectively from a centralized point [14]. Regardless of the cloud computing model adopted, an organization cannot outsource the responsibility of governance to a third party or even the CSP. Thus, organizations must verify and understand cloud security, carefully analyze the security issues involved and plan for ways to resolve them before moving workloads to the cloud [14].

3.2. Legal Framework

There are legal implications of cloud computing and organizations must therefore cover it and include it in their frameworks. Many organizations are mandated by countries of jurisdiction and/or industries to safeguard personal data and the security of information and systems and to comply with some codes of conduct. A requirement if flouted may subject an organization to financial losses in form of fines or loss of operating license. Cloud computing was regarded as global thinking, and establishing common rules is impossible [14]. This is supported by the various variations in regulations observed between countries, states, and industries. It is therefore pertinent that organizations extending their operations to the cloud would need to get accustomed to different regulations that may apply. Organizations for Economic Cooperation and Development (OECD) developed some fair information-sharing principles [14] but the harmonization of various stakeholder interests may not happen very shortly. In many cases, the laws of different countries might apply concurrently, by the following:

i. The cloud service provider's location
ii. The cloud service user/consumer's location
iii. The location of the data subject
iv. The physical location of the cloud underlying hardware/servers
v. The legal jurisdiction of the contract between cloud actors (including cloud carrier, cloud auditor, and cloud broker)), which may be different from the locations of any of the actors involved
vi. Treaties and/or other legal frameworks between those various locations.

Organizations therefore must seek to understand the applicable legal framework they are subject to by examining the jurisdiction of their operations, which law may apply, and see to understand and factor them into their planning to guard against financial losses.

3.3. Business Continuity and Management Planes

Business Continuity and Management Planes: The Cloud consolidates the administration of cloud services which were kept separate in traditional IT computing by systems, tools, and roles. The management plane is the consolidation of all resources and access. An unauthorized user gaining access to

the plane may have dire consequences for the organization. This is not to say that there is no benefit in the consolidation of access, resources, and roles but this may mean excessive access for certain categories of users. The management plane guarantees ease of access and resource administration. However, the compromise of such a sensitive account may have a devastating effect on an organization. It is, therefore, necessary for organizations to plan the limits and scope of the management plane right from inception and adoption of the cloud to minimize risk.

Other solutions such as zero-trust implementation and IAM may well be used to ensure business continuity while minimizing the risk of wide management planes.

3.4. Infrastructure, Application, and Data Security

It is critical to have a well-established dynamic security model for the infrastructure of the cloud computing [15]. CSPs have some set of out-of-the-box infrastructure security solutions available to cloud consumers to configure and turn on. Since the security defaults may not meet every organization's requirement, it is important to evaluate the cloud provider's security offerings to see if it meets the individual organizations' requirements. Where it does not meet the requirement, a third-party security service broker solution may be used to augment the solution provided by the CSP.

3.5. Incident Management

Security incident handling is an essential component of the security management [16]. It deals with the timely detection and analysis of security incidents, as well as the subsequent response (i.e., containment, eradication, and recovery). The existing incident response process for traditional computing can serve as input for cloud incident management. An effective incident management process for the cloud must cover all aspects of incident handling and response, with an escalation matrix and threat triage clearly defined and documented. Since risk/responsibilities are shared between the CSP and users, there is a need for alignment of cloud-service users to the laid down incident management procedure of the cloud provider to ensure smooth invocation of the response plan should there be a need.

4. Methodology

The methodology considered the secondary data from the Identity Theft Resource Center (ITRC) database [17]. Data relating to cloud incidents between year 2020 to 2022 were considered and analyzed for cloud-related incident trends over those three years. Descriptive statistics and trend plots were utilized in the data analysis to identify patterns and priorities the steps that organizations needed to take to protect themselves from common threats and control cloud risk. Since the focus of this work is on the public cloud, physical attack records related to on-premises/traditional IT were not considered.

Table 1. *Compromises by Attack Vector.*

	2022 YTD	FY 2021	FY 2020
Cyberattacks	1154	1613	878
Phishing/Smishing/BEC	343	537	383
Ransomware	194	352	158
Malware	60	141	104
Non-secure Cloud Environment	6	24	50
Credential Stuffing	14	14	17
Unpatched software flaw	-	4	3
Zero Day Attack	3	4	1
Other	19	426	162
NA - not specified	515	111	-
Systems and Human Error	100	179	152
Failure to configure cloud security	13	54	57
Correspondence (email/letter)	15	66	55
Misconfigured firewall	7	13	4
Lost devices or document	3	12	5

	2022 YTD	FY 2021	FY 2020
Other	5	34	31
NA-not specified	6	-	-

5. Discussion of Findings and Recommendation

The result of the analysis is as follows.

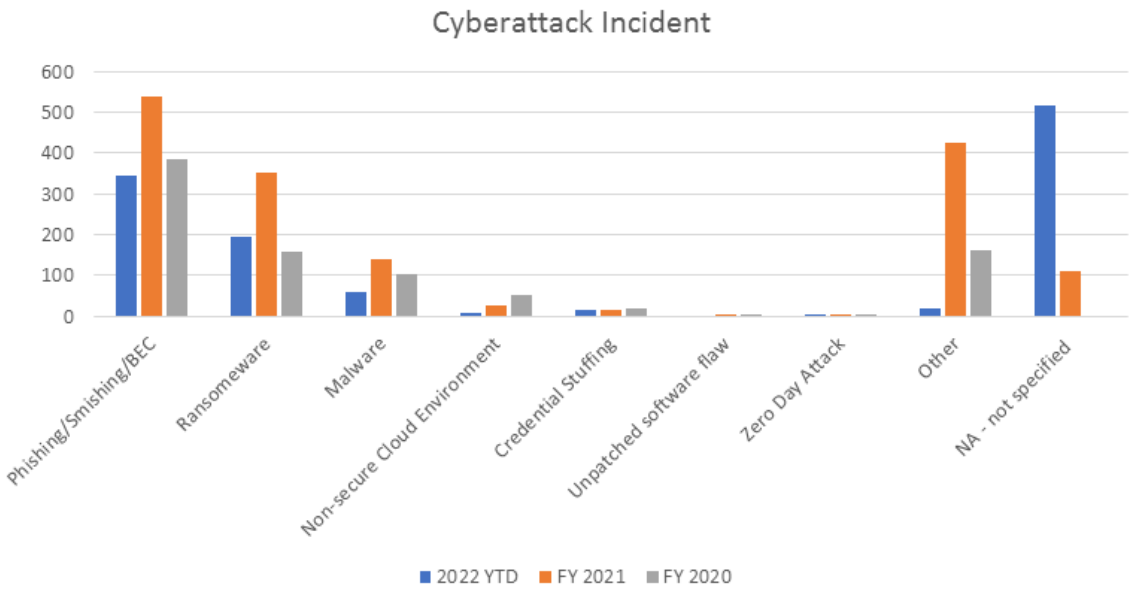

Figure 3. *Cloud Incidents distribution based on attack type.*

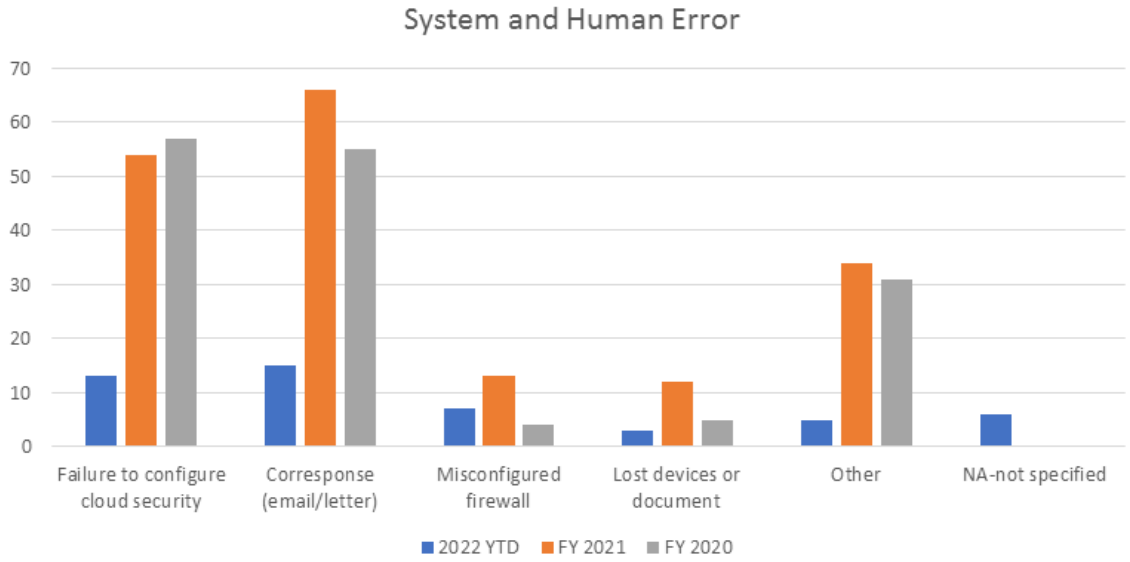

Figure 4. *Cloud incidents distribution based on system and human error.*

1. The analysis revealed that successful cyberattacks recorded against cloud computing rose in 2021 and had some decline in 2022. While a decline in cyber-attacks was recorded in 2022 when compared to 2021, it was however observed that phishing and ransomware attacks over the observed period have not reduced sig-

nificantly. Phishing and ransomware are not just a threat to the cloud, traditional IT is affected. Since phishing and ransomware attack evolves, and sometimes evade detection, effective user awareness, education, and training has been suggested as the next best method of protecting the business against such attacks [18].

2. Malware and lack of effective security control are also observed to have increased between 2020 and 2022. While the incidents related to malware and control breaches are not significant when compared to other incidents, they are totally avoidable. Control matrix and governance of cloud administration should be brought under the governance and enterprise risk management where it can receive focused attention [14]. Malware attacks can also be further prevented by ensuring effective endpoint security and other solutions are deployed. An assessment of the workload being run in the cloud against the security solution offered by the cloud vendor should be carried out. Where necessary, a third-party security solution should be used to supplement the offering from the CSP.
3. The availability of huge and uncategorized attack vectors signals a need for security architecture training. Some of the respondents of the survey by ITRC understood there was a breach but could not describe in detail what was observed. While attacks and threats are evolving, security professional training and education are highly important to stay current on the zero-day threats and be equipped with sufficient knowledge needed to defend the cloud infrastructure against cyber-attack. It is also essential that not only the IT administrators are certified on cloud computing in use, information security engineers, data protection officers, compliance officers and other roles within the IT risk management structure should be mandated before organizations begin setting up their footprint in the cloud.
4. Systems and human error are avoidable. Failure to configure cloud security and firewall misconfiguration may have stemmed from inadequate knowledge of the platform or a lack of proper change management process. Stakeholder education is required and where needed change management process should be introduced to guide every aspect of control changes in the cloud.
5. Organizations may also introduce proper governance of identity through the use of identity and access management (IAM) solutions and zero-trust implementation [19-21]. User accounts and devices are part of the security architecture of the organization, and if either of these is compromised, it can effectively weaken the security posture of the organization. The zero-trust architecture ensures that access to organization resource by devices and user accounts are not granted by default until such access is evaluated against established metrics.
6. Organizations must also take full responsibility for the security of their cloud computing. While cloud security risk and responsibility are shared between CSPs and users, most security breaches were seen to be a direct result of misconfiguration and knowledge gaps on the part of the cloud users.

6. Conclusion

The increased cloud computing use came with a big risk; the main disadvantages of cloud computing are security threats, a larger attack surface, privacy issues, and the inability to verify that CSPs are taking security seriously. However, the risk associated with cloud computing is not all that different from that of traditional computing. In the former case, organizations have complete responsibility and liability for the risks, whereas in the latter case, the CSPs and cloud clients share responsibility for risk.

The examination of cloud-related incidents from the ITRC database between 2020 and 2022 demonstrates that the majority of incidents are caused by knowledge gaps and the cloud customer's failure to exercise due diligence and care. Risk would be successfully reduced to a manageable level by following the established cloud control matrix, such as the CSA. Based on trends, the analysis also recommends that before shifting workloads to the cloud, users, cloud administrators, security engineers, and other roles within the IT risk management structure should be made aware of, trained in, and educated about cloud risk and the frameworks available to manage it.

Zero trust technology and IAM Solutions are also viable solutions to combating open access of lost devices and compromised user accounts.

To manage the risk and safety of computing in the cloud effectively, an organization must take responsibility for the risk associated with the cloud, have appropriate frameworks in place and implement controls before moving services to the cloud.

Abbreviations

CSP	Cloud Service Provider
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ITRC	Identity Theft Resource Center
NDPR	Nigeria Data Protection Regulation
OECD	Organizations for Economic Cooperation and Development
OEM	Original Equipment Manufacturer
PaaS	Platform as a Service
SaaS	Software as a Service
TCO	Total Cost of Ownership
NIST	National Institute of Standards and Technology

Author Contributions

Ayokunmi Ogundapo: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Project administration, Visualization

Vitus Nnamdi Ezeaputa: Validation

Conflicts of Interest

The authors declared no conflicts of interest.

References

[1] N. Caithness, M. Drescher, and D. William, "Can functional characteristics usefully define the cloud computing landscape, and is the current reference model correct? " *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 6, no. 10, 2017.

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology Special Publications*, Vols. 800-145, pp. 1-7, 2011.

[3] H. Ahmed, M. Ali, L. Kadhum, M. Zolkipli, and Y Alsariera, "A review of challenges and security risks of cloud computing." Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(1-2), pp 87-91, 2017.

[4] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud Computing Risk Assessment: A Systemic Literature Review" in Future Information Technology, vol 276, 2014.

[5] J. Hedman, and X. Xiao, "Transition to the Cloud: A vendor Perspective," 2016 49th Hawaii Internarional Conference on System Sciences (HICSS), Koala, HI, USA, 2016, pp 3989-3998.

[6] N. Daylami, "The Origin and Construct of Cloud Computing," *International Journal of the Academic Business World*, vol. 9, no. 2, pp. 39-45, 2015.

[7] A. Rot, "Data and Services Security Issues and Challenges in Cloud Computing Environments," in *22nd World Multi-Conference on Systemics, Cybernetics and Infomatics*, Wroclaw, 2018.

[8] M. Liangli, S. Yufei, C. Yanshen and W. Qungyi, "Virtualization MAturity Refernce Model for Green Software," *International Conference on Control Engineering and Commincation Technology*, 2012.

[9] L. Malhotra and D. Agarwal, "Virtualization in Cloud Computing," *Journal of Information Technology and Software Engineering*, vol. 4, no. 2, pp. 1-3, 2014.

[10] S. Goyal, "Public vs Private vs Community - Cloud Computing: A Critical Review," *International Journal Computer Network and Information Security*, vol. 3, pp. 20-29, 2014.

[11] M. S. R. C. (MSRC), "Investigation Regarding Misconfigured Microsoft Storage Location," Microsoft Inc., 19 October 2022. [Online]. Available: https://msrc-blog.microsoft.com/2022/10/19/investigation-regarding-misconfigured-microsoft-storage-location-2/ [Accessed 19 November 2022].

[12] S. Gatlan, "Microsoft data breach exposes customers' contact info, emails," Bleeping Computer, 19 October 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/microsoft-data-breach-exposes-customers-contact-info-emails/ [Accessed 15 December 2022].

[13] R. Mogull, J. Arlen, F. Gilbert, A. Lane, D. Mortman, G. Peterson and M. Rothman, "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," Cloud Security Alliance, 2021.

[14] F. Pfarr, T. Buckel and A. Winkelmann, "Cloud Computing Data Protection - A Literature Review and Analysis," in *47th Hawaii International Conference on System Science*, Hawaii, 2014.

[15] M. Yildiz, J. Abawajy, E. Tuncay and A. Bernoth, "A Layered Security Approach for Cloud Computing Infrastructure," in *10th International Symposium on Pervasive Systems, Algorithms, and Networks*, 2009.

[16] B. Grobauer and T. Schrek, "Towards Incident Handling in the Cloud: Challenges and Approaches," in *Cloud Computing Security Workshop*, Chicago, 2010.

[17] I. T. R. Center, "Q3 Data Breach Analysis," Identity Theft Resource Center, October 2022. [Online]. Available: https://www.idtheftcenter.org/publication/q3-2022-data-breach-analysis/ [Accessed 15 December 2022].

[18] J. E. Thomas, "Individual CyberSecurity: Empowering Employees to Resist Spear Phishinh to Prevent Identity Theft and Ransomeware Attacks," *International Journal of Business and Management*, vol. 13, no. 6, 2018.

[19] A. Kerman, O. Borchert, S. Rose and A. Tan, Implementing a Zero Trust Architecture, National Institute of Standards and Technology, 2020.

[20] I. Indu, R. Anand and V. Bhaskar, "Identity and Access Management in Cloud Environment: Mechanisms and Challenges," *International Journal of Engineering Science and Technology*, vol. 21, pp. 574-588, 2018.

[21] M. Armbrust, A. Fox, A. D. Joseph, R. Griffith, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Electrical Engineering and Computer Sciences, University of Califonia, Berkeley, 2009.