International Journal on Emerging Technologies **11**(5): 320-329(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Significance of Cloud Security Policies and Practices in Corporations and Organizations

Pratik Das and Nishant Kumar
[1]B. Tech, Department of Computer Science & Engineering,
Gurukula Kangri Vishwavidyala, Haridwar Uttarakhand, India.
[2]Assistant Professor, Department of Computer Science & Engineering,
Gurukula Kangri Vishwavidyalaya, Haridwar Uttarakhand, India.

(Corresponding author: Nishant Kumar)

(Received 29 June 2020, Revised 13 August 2020, Accepted 04 September 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The recent era of technological advancements in the IT field, has helped in developing new innovations and ideas to enhance and simplify the business workflow of various organizations and sectors. But, between an organization idealizing about migrating to cloud and actually taking their sensitive business data to a shared public platform, there are various factors that are needed to be considered thoroughly, like profit margin associated with migration, legal protocols to be followed and one of the most crucial aspect, i.e. the risk and security concerns of using a cloud platform for primarily running their business endeavor. In essence, the paper focuses on two major facets of cloud technology— first, the security concerns associated with migration and implementation of business on cloud and secondly, the facts & figures associated with the cost of breach, the cost associated with implementing secure cloud solutions, and the cost justification associated with it.

Keywords: Cloud security, Business Flow, Cloud Computing, Policies, Secure Practices, Compliance Models, Security Control, Return-of-Investment on Cloud.

I. INTRODUCTION

In the scenarios of mounting pressure on budgets and bottom lines, the ability of cloud solution to monumentally cut costs, is what drives the companies for cloud adoption. But, it is not the only reason why many businesses and organizations are shifting towards cloud. According to a recent analysis by CompTIA [37] in 2016, 47% of large enterprises and 41% of medium businesses and small firms migrated to a cloud solution. For these companies, the massive cost-reducing factor of cloud outweighed other factors like speed, modernization and complexity reduction.

Primary factors leading to migration are :

- Cost
- Security and Compliance
- High availability of resources
- Reliability
- Scalability and Application Support

— What is meant by the term "Cloud Computing"?

The unique innovation of combining grid computing, along with the prowess of parallel and distributed processing, gave birth to this revolutionizing technology, which is known as Cloud Computing today.

It is a service of dynamically provisioned resources backed by interconnected and virtualized computers, provided to client under the conditions negotiated with the provider in Service Level Agreement (SLA) [1].

A large pool of easily accessible and usable resources, it realizes the concept of provisioning IT infrastructure, made up of virtualized hardware platform, for high-speed, scalable and cost effective utility computing, on demand.

This concept dates back to early 1960s, when it was suggested by Professor John McCarthy that the time-shared computing resources would become commercial in the future [2]. Even back in the 70s and 80s, the symbol of "cloud" was often used to depict components in various Network Structure Diagrams in the ARPANET and CSNET. In 1993, it was referred to as a platform for "distributed computing". Not until the year 2006, the term "Cloud Computing" was popularized, when Amazon unveiled their product "Elastic Compute Cloud" (EC2) [3].

Amazon Web Services (AWS) revolutionized the field in 2002, when they upgraded their data centers and started the provision of their systems to users on utility computing basis [2]. After the introduction of cloud computing to the world, the availability of low cost and high performance resources on-demand became a boon for many businesses and corporations. Soon, this technology would be used for migrating innumerable conglomerate's solutions and application to a more accessible, scalable and cost-efficient platform.

— Interest of Corporations in Cloud Computing from a Business Perspective.

The onset of cloud-driven era had many Business heads and associates asking salient questions like

- "What is the market opportunity for this technology?"
- "What is the future potential for the long-term utilization of it?" [2]

After the modernized approach devised for the delivery of cloud services on demand, companies witnessed multitude of benefits in their business process cycle. For instance, now that the cloud resources are being shared with multiple consumers, rate of utilization peaked as all servers were being used at one time or the other, none of them went idle.

This also resulted in immense saving of infrastructure cost. Also, added benefits of high- speed bandwidth along with inexpensive computer power advanced the cause of multitudes of conglomerates and businesses, helping them expand their solutions to clients, that too, with several financial profits.

— "With great technological advancements, come crucial security concerns as well."

Any new technology, in its newly developed phase, goes through persistent development, rectification for its growth. Being an innovation in its field, it is often vulnerable to vast possible risks. Cloud technology is also is in its emerging phase, advancing eventually, but still prone to security threats and possible hazards. Cloud computing went mainstream in the early 2000s, but its full potential is yet to be harnessed. According to Cisco System, Inc., it is estimated that 94% of the business workload will be in cloud by the year 2021 [4].

With rapid development already in progress for cloud services, a considerable issue that still remain is, that whilst focusing on advancement in cloud technology, security aspects pertaining to it might be overlooked; which might become a fatal issue in the time being. Unlike the issues occurring in the enterprise setting that can be contained without attracting negative publicity, issues occurring in the public cloud environment receive a lot of public exposure, which in turn, makes it to the headlines, thus generating a bad reputation for the organizations associated as well as the cloud technology itself. If not handled and maintained with utmost caution, cloud services can face potential dangers of

- Data breaches
- Data loss
- Denial of Service
- And more.

Such factors can eventually result in a business facing irrecoverable compromise of their resources along with disruption of the business workflow, tremendous amount of financial loss and colossal damage recuperation prices. To top this off, the company might lose trust of their customer base ("abnormal churn") and may face the wrath of extensive lawsuits or legal repercussions from agitated clients and concerned stakeholders.

A. Importance of Practicing Safe Cloud security policies

Provision of cloud service models to innumerable clients, whose purpose is to store hefty amount of data while being concerned about their user privacy, identity and application specific preference in centralized location, inadvertently raises many apprehensions about data security. To counter the persistent issue of data security, the concerned parties should consider implementation of legal framework to protect their interests and privacy, without compromising on the key features of the cloud services. This is where security policies and compliance models step in.

Standardization is one of the most quintessential aspects determining the adoption of cloud computing models by the consumer. Many standard bodies are in works of proposing a cloud security standard, for instance, Cloud Security Alliance (CSA), National Institute for Standards and Technology (NIST) and International Organization for Standards (ISO) [5]. They are in dire need of being finalized before cloud computing becomes ingrained in daily public lives. Now-a-days, many cloud safety measures, pertaining to a specific cloud service delivery model, are provided by Cloud Service Provider themselves. This paper's focus is to shed a light on cloud computing and security practices associated with it, along with instances of security measures various big conglomerates deploy around their cloud services to keep their client's data safe and secure. The paper will enlighten its readers about necessity of practicing robust security policies with exemplar cases from real world, along with insight of financial statistics involved in deploying these policies.

II. PREVIOUS RESEARCH

Privacy of client's data has been one of the chief concerns from the beginning of commercialization of cloud computing. There are various facets regarding privacy and its preservation, for instance –

- Who has the authority to access the data stored on the cloud server?
- Can a service provider access the cloud's data without the client's consent?
- Do cloud service providers, access user's stored sensitive data without user's consent?

Privacy is the key market differentiator in today's cyberworld. Dr. Larry Ponemon, founder and chairman of CIPP, while emphasizing on the importance of online privacy in the climate of decreased trust, stated that, "Consumers want to do business with trusted service provider they believe they can trust" [2].

Previous studies have also made an effort to determine and address the issue of cloud security and standardized policies. For instance -

Zissis et al.'s work focused on associating and evaluation of key security requirements related to cloud security issues; and proposed a solution efficiently concerned with an entrusted 3rd party to secure the essential characteristics of the cloud architecture [6]

Joshi *et al.* work emphasized on a more semantic methodology of solving the cloud security issues. A framework for determining security threat classification was proposed, along with associating it with a suitable compliance control required to mitigate the issue and the cloud providers supporting those compliance standards [5].

Buhl *et al.,* research concentrated on issues faced whilst implementing a secure cloud solution and also proposed key security features to be provided by every cloud solution for data integrity and privacy (provision for multi-tenancy with iron-clad isolation for each tenant, providing incorporation with tenant's organization security policy etc) [7].

But there are still steps required to be taken for a standardized approach to cloud security. Following best privacy practices significantly results in improved business, but this is usually enforced by legal policies and compliance controls in place. Various countries have enacted several laws to identify citizen's right to information privacy and to protect the same. For instance –

- Canada has Personal Information Protection and Electronic Documents Act (PIPEDA) [2].
- European commission's directive of data privacy, such as Swiss Federal Data Protection Act (DPA) and Swiss Federal Data Ordinance Act [2].
- United States of America follows the Health Insurance Portability and Account- ability Act (HIPAA) [2].
- General Data Protection Regulation (GDPR) is law for protecting citizen's right to privacy within European Union [8].

The following sections will present the instances of cloud security policies and compliance controls followed by conglomerates and organization, and a stark analysis on “cost of a breach” and “cost-to-profit return” on using secure cloud practices.

III. CLOUD SECURITY POLICIES AND COMPLIANCE CONTROLS

This section will focus on key features that exemplar companies, dealing with cloud- enabled solutions/platforms, actually imbue in their Modus operandi.

Case 1: UnitedLex Corporation

A private independent service-based company, UnitedLex Corporation is a conglomerate which provides legal services in the field of litigation, document review, intellectual property and cyber-risk solutions. Founded in 2006 with its current Chief Executive Officer Daniel Reed, the company has striven effectively to migrate their business solutions and data to cloud in a secure manner for an improved efficacy of their services, while trying to find the right balance between advance technology implementation and the legal aspect surrounding it. The company has taken a radical and holistic approach for cyber threat mitigation in perspective of their business continuity, which is “defensible, adaptive and actionable” in nature [9]. The organization is devoted to providing cyber-risk solutions and believes in pro- viding their clients, an adaptive program for advanced preemption of risk and threat, which also maximizes their figures of Return of Investment. They provide the following service components in their cyber-risk division -

- Risk Assessment and Strategy Development —They recognize critical data assets, evaluate threats and define a strategy for the client, to manage their unique risks, and optimally prioritize security resources and investments. This also includes: Critical Data Asset Risk Assessment, Vulnerability Detection and Penetration Testing, Third- party Risk Assessment and Monitoring [10].
- Incident Response and Forensics - A dedicated team of experts responding to any kind of security incident and the client works with a team that understands how to manage the forensic, legal, IT operations and risk management aspects of a potential data compromise dramatically reduces the impact of an incident. This service focuses on: Incident Response Services, Incident Readiness Assessment and Playbook Development, Compromise Assessments, Malware Analysis, Advanced Net- work Forensics and Expert Reporting [10].
- Managed Detection and Response (MDR) — With their monitoring tools and security analysts on duty, the organization provides their clients with an active network security monitoring solutions for ensuring the safety of the enterprise’s network. Moreover, following aspects are also catered: SOC (Security Operations Center)-as-a-Service, Managed SIEM, User Behavior and Security Analytics, Endpoint Threat Detection and Response (ETDR) [10].
- GDPR Compliance — Following the recent passing of the stringent law, which dictates the regulations for handling and protecting the private data and Personally Identifiable Information (PII) of EU citizens, the organization have redefined and enhanced their programs and policies to be more amenable and compliant to GDPR compliance policy. Moreover, UnitedLex GDPR Readiness Consulting Services provide leadership and support for your internal efforts to create a practical and sustainable GDPR program. Also, UnitedLex has designed a suite of services to extend support to organizations that seek outside assistance in fulfilling DPO (Data Privacy Officer) obligations under GDPR policy [10].

Following are some quintessential facets of security practices followed by UnitedLex Corporation –

- ISO/IEC 27001:2013 Certified; Follows Information Security Management System (ISMS) to the core for securing people, process and IT infrastructure by applying a risk management process [11].
- Compliance with regulations and industry guidelines, such as HIPAA, GLBA, GDPR, PCI-DSS, ISO 27001/2, NIST Cybersecurity Framework [12].
- Provision of “State-of-the-art” Managed Security Services to help clients assess and monitor their resources more efficiently [13].
- Involvement of stakeholders from across the organization, in context of Managed Security Service Provider (MSSP) services, and thorough comprehension of the nature of client’s business, end user behavior and data to tailor a security program to satiate the organization’s business and legal needs [13].
- Development of Consultant led technology-enabled service “Questio” combining targeted automation, legal intelligence and data analysis. Reduction of data and cost while improving both the timeliness and efficiency of data analysis and document re- view. This document reduction yielded the client costs savings (on average) from 40% to 50% per matter [14].
- Managed Detection and Response (MDR) leverages cloud for consuming the event data and also as an event resource. MDR uses industry leading network and endpoint threat detection sensors to detect anomalous traffic and processes [10].
- Usage of Artificial Intelligence applied to the entire log generated across client’s environment – Intrusion Detection Service logs, Intrusion Prevention Service logs, Anti-Virus logs, Firewall logs, Syslog data etc. [15]
- UnitedLex SIEM Triage provides comprehensive review of client’s configuration for checking and verification of compliance logging and required threat detection [12].
- Deployment of a Rapid Response (R2) platform to monitor and secure the client’s infrastructure and business environment and significantly help in decreasing risk mitigation and incident response time [16].
- Integration of Cloud Access Security Broker (CASB) or Web Application Fire- wall (WAF) in MDR services [17].
- Deployment of Endpoint Threat Detection and Response (ETDR) tool in client’s environment, or co-manage it with the client’s existing ETDR tool (like Carbon Black) and Deploy ETDR sensors in both physical and virtual devices [10].

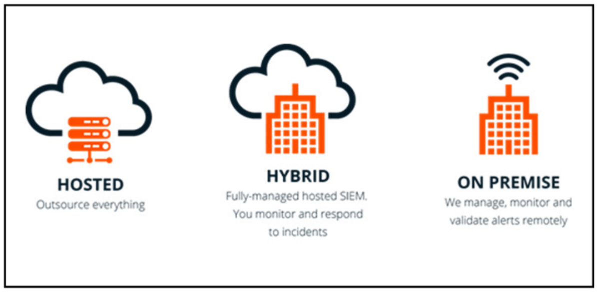
HOSTED
Outsource everything
HYBRID
Fully-managed hosted SIEM. You monitor and respond to incidents
ON PREMISE
We manage, monitor and validate alerts remotely

Fig. 1. UnitedLex SIEM[12].

UnitedLex' s strict adherence to ISMS policy in their trade and code of conduct is one of the prime reason ensuring security and diligence of their cloud-based Cyber-risk solutions and other business processes.

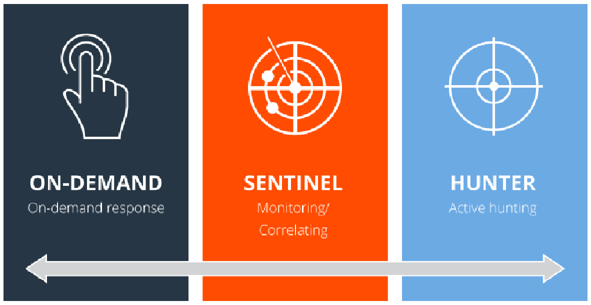

Fig. 2. Rapid Response Platform [16].

Case 2: IBM Corporation (International Business Machines)

IBM Corporation is an American public multi-national company, providing IT consultancy and services, along with cutting edge cloud and cognitive computing on-demand. Operating over 170 countries, it is headquartered in New York, United States [18]. It is currently rated as #3 in all Cloud Vendors, dethroning Sales force and SAP to #4 and #5 respectively; and is succeeded by Amazon Web Services and Microsoft.

IBM markets computer hardware, middleware, software and provides hosting and consulting services in areas ranging from mainframe computing to nanotechnology. It is also one of the leading organizations in research and patents, and is accredited with the most amounts of U.S. Patents generated by a business.

Along with their various services, IBM Corporation strictly follows and adheres to security policies and implementation guidelines provided under their binding commitment to Data Security and Privacy Principles. Following are some of the Compliance conformed by IBM Cloud –

- ISO 27001 — Outline requirements for Information Security Management System [19].
- ISO 27017 — Provides guidelines for Information Security Controls for Cloud service provision and usage [19].
- ISO 27018 — Establishes commonly accepted guidelines, objectives and objectives for protecting Personally Identifiable Information (PII) [19].
- ISO 22301 — Provides requirements for implementing, maintenance of Business Continuity Management System (BCMS) [19].
- ISO 31000 — Principles, frameworks and process for Risk Management practices [19].
- SOC1, SOC2 and SOC3 — Provides controls at service organization useful to user entities and auditors for planning a financial statement audit and evaluating internal control [19].
- PCI — To protect cardholder's data, often requires validation from 3rd Party Qualified Service Assessor (QSA) [19].
- HITRUST — Maintains certifiable framework to help healthcare organization demonstrate their security and compliance in a consistent manner [19].
- FedRAMP — A standardized approach to security assessment, authorization and continuous monitoring of cloud services and products [19].
- IRAP (Australia) — Framework to endorse private and public sector individuals to provide cybersecurity assessment services to Australian government [19].
- IBM ISO Management System Certification — Compliance with ISO 9001, ISO 14001, ISO 50001 and OHSAS 1800 [19].

Also, with this, IBM also serves strict adherence to many Global Regulations such as EU Model Clauses, FERPA, HIPAA (U.S.), My Number Act (Japan), ITAR (U.S.) and Cloud Computing Compliance Controls Catalog (Germany). Along with this, the conglomerate follows alignments and frameworks in accordance to these organizations and acts

Criminal Justice Information Systems (CJIS) Division, Cloud Security Alliance (CSA), Federal Financial Institutions Examinations Council (FFIEC) and Federal Information Security Management Act (FISMA).

The following represents some of the essential security aspects in Cloud Services followed by IBM Corporation.

- IBM deploys encryption solutions like CloudLink, Secure VM, IBM Cloud Data Encryption Services (ICDES), Project V and KeySecure from SafeNet to ensure stringent encryption of data-in-transit and data-at-rest [20].
- Usage of cloud native and vendor solutions by IBM, such as IBM cloud VLANs, Vyatta Gateway, Fortigate Firewall and Citrix NetScaler to let administrator guarantee multi-layered security for Network zone Segmentation, Partition and Provision of Routing and Filtering Needed to isolate users, domains and workloads [20].
- Deployment of IBM Solutions like QRadar, XForce Threat Analysis Service and Hosted Security Event and Log Management Service for managing the security policies for private and public cloud environment [20].
- Using solutions from vendors like CloudPassage, Sumo Logic Observe IT to automatically define policies around firewall rules, file integrity, security configuration, access control and to audit adherence to such policies [20].
- Authentication on IBM Cloud using IBMid for Identity Access and Management [21].
- Single sign-on on IBM Cloud, leveraging industry standard protocols such as SAML [21].
- Encryption of content not intended for public or unauthenticated viewing, whilst using cryptographic protocols such as HTTPS, SFTP, FTPS etc. for Client's secure transfer of Content to and from Cloud service over public network [22].
- Usage of following combinations of encryption and data integrity algorithms in IBM Cloud Object Storage:

RC4-128 and AES-128 encryption with MD5-128 Hash for data integrity. [21]

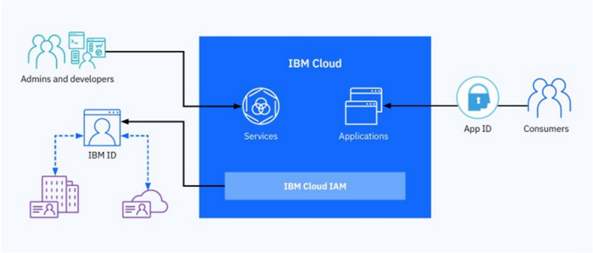

Fig. 3. Identity Access and Management in IBM Cloud [23].

IBM's scalable suite of technology and solutions are made more robust with the imminent help of pervasive encryption, Artificial Intelligence automation and integration. With end-to- end security implementations for both cloud-native and enterprise applications and data, IBM ensures that the client's sensitive data is thoroughly protected within (but, not limited to) the bounds of Confidentiality-Integrity-Accessibility Triad.

Case 3: Cloudflare Inc.

Cloudflare Inc. is a website performance and Security-as-a-Service provisioning company which was found in 2009. It is a Private, Independent company in IT industry sector, currently headquartered in San Francisco, California, U.S.

The founders' (Matthew Prince) prime intention was to track how spammer harvested e-mail addresses for Bulk E-Mail spamming, which led to the birth of Project "Honey Pot". The simple and efficient project thrived and improved over the years, and helped in tracking innumerable adversities for website administrators. On consumer's demand, in due course, they moved on to stopping and averting the aforementioned threats, rather than just tracking them [24].

CloudFlare specializes in the following services –

- Content Delivery Network (CDN) — Network of one of the largest Internet ex- changing point, they cache the content across their global network, thus improving connection, reducing speed of request and fastening application response time via improving cache hit ratio [25].
- Distributed Denial-of-Service (DDoS) Protection — Mitigation of advance at- tacks, and protecting the clients from highly distributed volumetric attacks which interrupts Business Continuity and costs Server downtime [25].
- Domain Network System (DNS) — Provision of free and one of the fastest authoritative Domain Name System service for clients managed by Any cast network and a 'first-of-its-kind' privacy-oriented consumer DNS service hosted at 1.1.1.1 and 1.0.0.1 [25].
- Reverse Proxy — Retrieval of resources from the internet on behalf of the client as an intermediary. [25]

The organization has the following security policies –

- The company is in accordance to the following frameworks and compliance: PCI (Privacy of cardholder's information), EU-US Privacy Shield (For international information transfer), GDPR and more [26].
- Layer 3 (120 Gbps traffic), Layer 4 (400 Gbps traffic) Layer 7 (1 Tbps traffic) DDoS Protection, with the help of its state-of-the-art Web Application Firewall [27].
- Rate-limiting and fine-graining of incoming traffic via configuring the request thresh- old and presenting challenges and CAPTCHAs; protection against any kind of abusive behavior targeting application layer [27].
- Provision of enhanced performance without compromising on security, Cloudflare Inc. increases application performance due to low-latency security services integrated with traffic acceleration [28].
- TLS 1.3 Support and Global Session Resumption reducing round trip amount [28].
- HTTP/2 speeds up page load times [28].
- Global Anycast network with 116+ data centers absorb highly distributed attack traffic [29].
- DNSSEC verification of DNS records using cryptographic signatures, thus mitigating the possibilities of cache poisoning or "spoofing" tricks [28].
- WAF examines web traffic for suspicious traffic, even filters it based on examination of GET/POST HTTP requests, rulesets such as ModSecurity core rule covering the OWASP Top 10 vulnerabilities and even updates the rules based on threats identified from 6 million customers [28].
- CDN is built with advanced optimizations, including auto-minification of HTML, CSS, JavaScript and Gzip compression, saving 20% on the size of files and resources [30].
- Cloudflare uses Argo Smart Routing Algorithm to reduce internet latencies [30].

Via provisioning fast cache-hit ratio (due to Full Page Caching methodology) and tough, all-round protection from stringent amount of attacks and possible breach or infrastructure downtime, CloudFlare offers effective solution as a Security-as-a-Service provider, mitigating any threats faced by their clients or customer immediately.

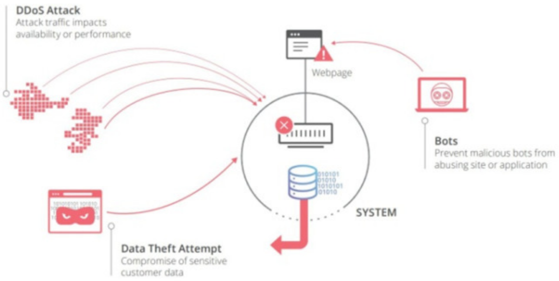
DDoS Attack
Attack traffic impacts availability or performance
Webpage
Bots
Prevent malicious bots from abusing site or application
SYSTEM
Data Theft Attempt
Compromise of sensitive customer data

Fig. 4. DDoS Attack [28].

IV. FACTS AND FIGURES — CLOUD SECURITY FROM BUSINESS POINT-OF-VIEW

The concerns and issues regarding business migration to cloud are always convoluted in nature, considering how there are ample of factors to contemplate before the company think about transitioning to the cloud. Even after the security aspects in consideration are thoroughly discussed over by the companies, there's another facet of migration that is heavily considered and decides whether the organization will move forward with the migration or not. And that is "Cost" — Cost of Breach, Cost of Expenditure on implementing a cloud infrastructure/cloud security policy in a conglomerate and return of investment. Essentially, when it comes to cloud computing adoption, money is still one of the quintessential motivators.

A. Cost of Breach

Equifax's 2017 Data Breach

The 2017 mega breach of Equifax led to compromise sensitive and financially crucial data of about 150 million customers [31]. In the aftermath, the company spent around $243 million [31] and counting for the damage recuperation and will probably spend millions more for the coming quarters on clean-up.

The Result? The company faced a massive abnormal churn (loss of customers and trust erosion after the event) and the CEO, along with some more involved high executives resigned within a week of the occurrence of the breach. [31]

Target's 2013 Data Breach

Compromising about 70 million people's [32] payment card and contact data, Target paid $19 million [32] alone for multistate settlement of lawsuit, not to mention the $10k compensation fee [32] paid individually to every customer affected by the credit-card data breach.

The aftermath witnessed the resigning of the CEO, few months after the data breach and the company continued to face tremendous amounts of lawsuits for the next few years [32].

Few more intriguing cases of data breach repercussions

The aftermath of TalkTalk data breach witnessed loss of more than 1 hundred thousand customers [33].

Yahoo Inc. had to lower its purchase price by $350 million in its acquisition by Verizon Inc [34].

I. Factor Analysis

These cases make a strong point and vehemently emphasizes that security is not something to be taken lightly. Along with surreal damage figures incrementing day-by-day, many higher officials and management personnel are also losing their occupation over it. In the cases of a data breach, the following factors strongly influence the damage price estimation

— Erosion of customer's trust followed by immediate loss of customer base.

— Expenses for upgrading IT infrastructure and security.

— Paying heavy legal fees and settlement to government and other organizations.

— Drastic toll on company's stock price.

— Professional impact on management teams (Chief Officers and other member's resignation and more).

— Other unspecified tangible and intangible costs.

Figures associated with the cost of breach

According to an intensive study conducted by Ponemon Institute in collaboration with IBM Corporation in 2018 (2000+ IT, data protection and compliance professionals from 477 companies), following figures were tabulated about data breach –

On A Global Scale $3.86 million is the average cost of data breach. $148 is the average cost incurred by company per stolen/lost record. 27% is the likelihood* of a recurring material breach in company in over the next 2 years [35].

On A Regional Scale South Africa has the highest possibility of future data breach recurrence (43%). Germany has the lowest possibility of future data breach recurrence (14.3%). The Per Capita Cost of Breach in U.S. and Canada are the highest ($233 and $203per record, $85 and $55 higher respectively than the global average). The Per Capita Cost of Breach in Turkey and India are the lowest ($68 and $67 per record, $80 and $81 lower respectively than the global average).The Average Data Breach Cost in U.S. is the highest ($7.1 Million). The Average Data Breach Cost in India and Brazil is the least ($1.7 and $1.24 Million respectively) [35].

The recent report by IBM [42] mentions that the average cost of a targeted breach, has amplifiedto an all-time high figure of 4 million 41 thousand U.S. Dollars. Report states that threat actors are leveraging misconfigurations as an initial foothold vector in the cloud infrastructure for gaining entry.

The study also emphasized that, Frequency of data breach according to industries has seem to hit the Financial and Services Industry the most, while the Education and Entertainment Industry remains the least frequently affected. Mean time to identify (MTTI) a data breach incident was estimated to be around 197 days. Mean time to contain (MTTC) a data breach incident was estimated to be around 69 days. The companies who were able to contain a breach in less than 30 days saved over$1 million against those who took more than a month.

In the recent report by Ponemon Report, companies laced with security automation also reported a significantly shorter MTTC response time, another essential cause shown to reduce breach costs in the analysis. Using machine learning, artificial intelligence and analytics facilitated the businesses response to breaches to be over 27% faster, than other businesses [42].

The root causes of breaches are Malicious or Criminal attacks (48%, Costliest of all data breaches), System glitch (25%) and Human error (27%, least costly of all data breaches). These factors tend to decrease the data breach cost - [35]

— Extensive use of decryption

— Appointed Chief Information Security Officer/Chief Privacy Officer

— Extensive use of Data Loss Prevention (DLP) scheme

— Participation in threat sharing

— Employee training

These factors tend to increase the data breach cost - [35]

— Third party involvement

— Compliance failures

— Increasing the use of mobile platforms.

B. Cost associated with implementing and maintaining cloud solution and cloud security practices in an organization

Seth Robinson, Sr. Director of Technology at CompTIA stated – The role of IT team is not to simply implement a cloud component to perform discrete function(s), but to drive business objectives forward by utilizing the right mix of cloud solutions. Cloud offerings can deliver cost efficiency, along with simplifying workflow and speeding up operations" [36].

Following are some diagrams representing the facts and figures associated with breach expenditure and factors leading to migration.

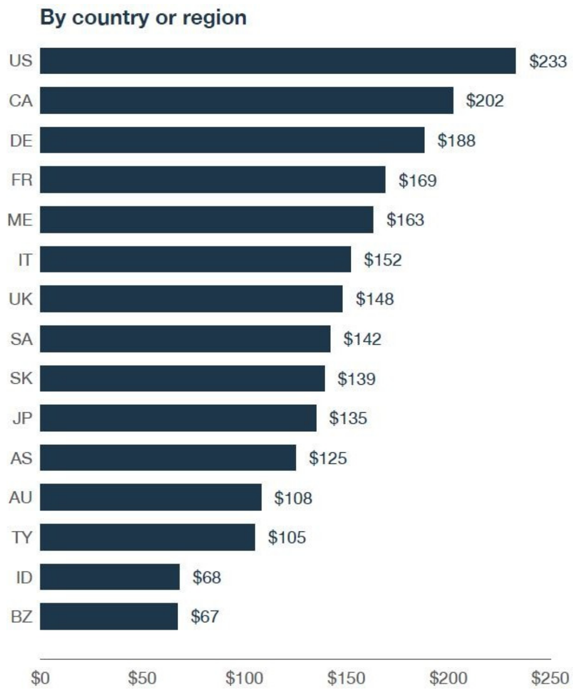

Fig. 5. Per Capita/Per Compromised Record Expenditure on Data Breach [35].

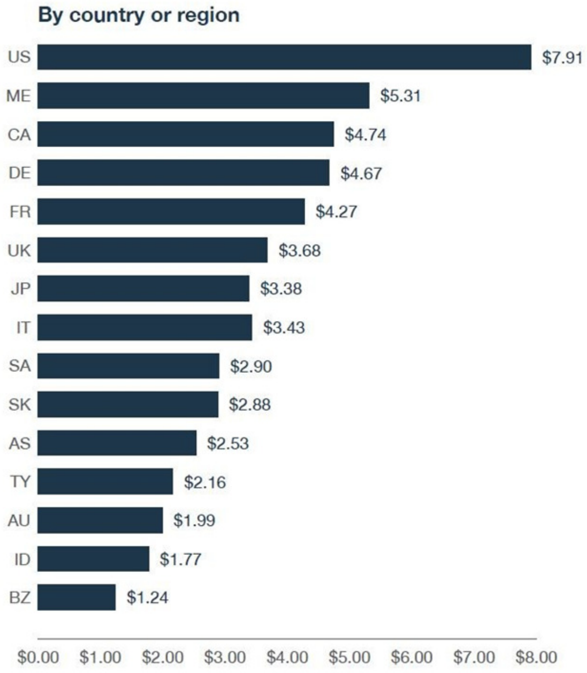

Fig. 6. Average Expenditure on Data Breach. (Figure in Million USD) [35].

In an intensive survey conducted by Cloud Endure, 50% of the companies surveyed estimated the cost of migration to be in between $100-$500/machine and 17% estimated that it costs more than $500/machine. Among enterprise companies, 23% estimated that it cost more than $500/machine to migrate to cloud [38].

All these statistics points to an evident fact — Cloud computing represents a larger and larger percentage of overall IT spending.

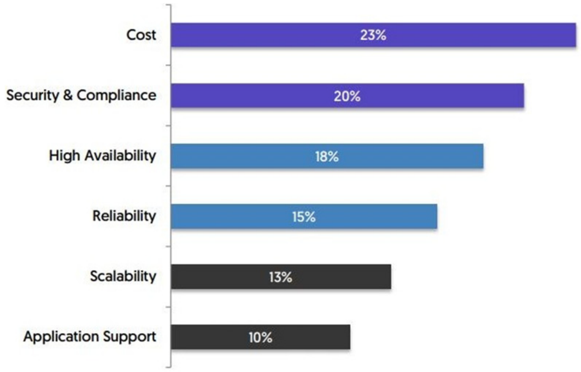

Fig. 7. Factors leading to Cloud Migration [38].

Following are the factors that affect the cost of implementing a cloud solution/security practice in a business [36].

- Moving large volumes of data to public cloud services and storing that data for a long period of time ($10,000-$100,000 per year).
- Network bandwidth accounts for much of the cost of moving data, as cloud providers charge upload and download fees.

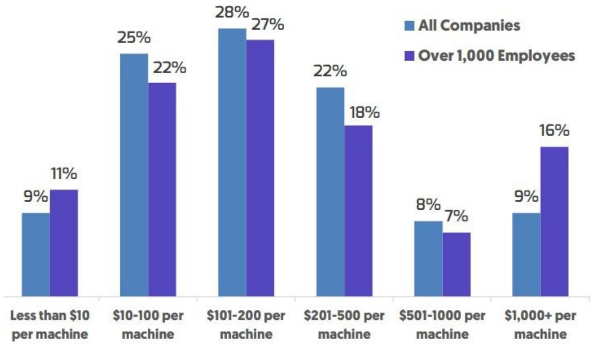

Fig. 8. Expenditure per machine [38].

- As companies scale-up to handle more workload, there's increased complexity in man- aging large servers. Similarly, handling amplified workload by virtual instances on cloud requires internal labor, which also incurs significant charge.
- Direct on-going costs: Choosing a business appropriate cloud service model(s) in accordance to company's work agenda and requirements; its subscription and transaction cost.
- Deployment and maintenance cost of the cloud solution — hiring experienced personnel or outsourcing the task.
- One-time migration costs: Ensuring proper migration, integration of the platform along with the porting of the applications
- Different costs of software/application integration varying from vendors to vendors.
- Testing the applications before migration conjures unforeseen costs — stabilizing system within cloud, which are already supporting various virtualized instances; figuring out which operating systems and databases would work.
- Risk management: Cost of downtime; adapting policies to avoid compliance issues and security
- IDC has predicted that $162 billion worldwide would be spent on public cloud by 2020. Deloitte projects

$547 billion in global spending on “IT-as-a-Service” by the end of 2018 [37].

Arguably, cloud computing solutions have proven to be one of the effective ways for a conglomerate to optimize and improve their business operations, while weeding out the unwarranted expenditures. Yet, without analyzing the cost-of-justification factor, it is impossible that one might even think about migration. The next section profoundly talks about the figures and facts revolving around Return-of-Investment in Cloud migration and security policy implementation and also discourses several factors involved in the profit statistics achieved due to cloud.

C. Return-of-Investment/Cost-of-Justification (ROI)

Whenever a company decide to migrate their business to cloud, they prioritize on developing a recommended cloud strategy, and choose between an on-premise solution and a cloud solution. The amount of workload an organization needs to handle, along with the revenue that they generate, defines their choice of strategy.

At the highest level, a conglomerate is concerned with the financial profit their decision can yield. Other factors, like cloud scalability, security and efficiency are also of quintessence, but it ultimately lies as a trade-off between these factors, and overall, they are the same reason why cloud migration seems like an enticing opportunity to various businesses.

While investing in cloud practice/cloud security policy, the Return-of-Investment factor is majorly based on these benefit areas –

— Cost reduction

— Improving Business Process Outcome

— Possible data breach mitigation

— Cloud platform providing Scalability

— Productivity enhancement

— Revenue transformation (re-investing the profit yield into more revenue generating activities)

For instance, Amazon has validated that even a slight 100ms speed improvement in the application process can yield an increase in sales by %1 [39].

In lieu of the factors affecting the Return-of-Investment, the CITO Research states that factors like [43] –

— Changing to Operating Expenditures from Capital Expenditures resulted into improved savings, in the context of “Pay-As-You-Go” for several businesses.

— Using Open Cloud assists in increasing the options of your cloud vendors for innumerable services. This significantly reduces the issues of a vendor lock-in.

An IDC study on the value of Performance-as-a-Service (PaaS) involving 10 companies and 1,190 users found that conglomerates developing and implementing custom applications on “Force.com” realized a total benefit of $8.21 for every $1 invested, and a 3-year Cost-of-Justification of 721% [40].

Consider the following case study of implementing load-testing solution.

Case Study: On-premises platform Vs. SaaS on-demand platform

- On-Premises load-testing solution:

This test was conducted for 120 executions per year. Any vendor of load-testing suite charges an initial license charge of approx. $300k + annual maintenance fee of $60k [41]. It also requires an additional user load-testing tool license per server. Along with this, it requires constant troubleshooting and maintenance by performance engineers (requires $60k per annum) [41]. According to 5-year cumulative observation, it was deduced that an organization depending on “On-premises” load testing solution yielded an estimated negative return figures ranging from 58% to 69% [41].

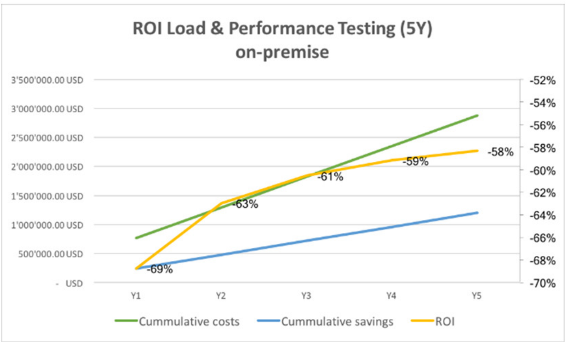

Fig. 9. ROI Load and Performance Testing: On-Premise [41].

- 4.3.1.2. Software-as-a-Service (SaaS) on-demand load-testing solution:

This test was also conducted for 120 executions per year. In this case, the service provider delivered maintenance and operation services for both load-testing software and underlying infrastructure and hosted the load agent machine. The organization only pays for their test results of load testing and actual usage of virtual resources. As no manual maintenance effort is required, it also helps in reducing headcount of an organization’s load and performance testing team to 4. Also, there is 20% decrease in defect occurrence in production [41]. Henceforth, the 5-year cumulative figures show that SaaS on-demand solution help realize 12% positive return on the investments [41], as there is no licensing cost involved, no requirement of maintenance effort and infrastructure.

The significant return figures on quarterly sales of any organization are enough to entice the high-level executives for taking the big step to the cloud. High performance improvement, along with increased sales gives the decision of migration an easy pass as a part of approval process.

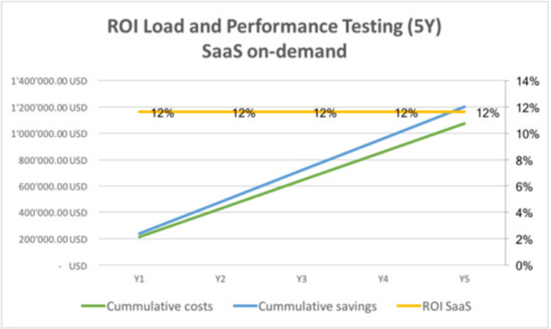

Fig. 10. ROI Load and Performance Testing: SaaS on-demand [41] .

V. FUTURE SCOPE

With respect to the paper’s context, the following aspects of cloud security and services can be an essential part of future scope -

— New expectations are being placed by cloud on the infrastructure, and with that, data integrity, confidentiality, and available must be guaranteed. While, these services are usually provided from the vendors itself, in order to make it all manageable and easy for customers, cloud vendors should provide products and tools which helps in managing visibility and control across assortment of cloud platforms.

— Businesses hosting their data and assets on a platform like cloud, tend to be concerned about the repercussions and consequences. There are several factors to be considered, like if the cloud vendor's security is up to their expectations or standards? Can the cloud platform be exploited for unauthorized access of data? Even the minutest of the minute entry point can provide a foothold for theft and illegitimate access. This makes access and authentication controls even more crucial in a platform like public cloud or shared cloud infrastructure, where attacks targeted at cluster can lead to compromising of numerous customer's assets. In such scenario, the cloud provider must offer a variety set of defense and security solutions centered on cloud platforms, facilitating to protect critical interfaces – between physical and virtual cloud platforms, the end users, and across private and public services running in the infrastructure.

— The purpose behind adopting a cloud platform for business processes is to minimize the cost of in-house business operations and optimize the processes, without compromising on any of the end-user features and functionality. The cloud service providers should strive to achieve the purpose by utilizing technologies like smart cloud management software, running on inexpensive commodity disks and servers.

VI. CONCLUSION

This paper attempts to present the perspective of cloud migration and adaptation by conglomerates from security as well as business point-of-view: What are the risks involved in cloud? Why is it necessary to practice safe security measures while adapting to cloud environment? What are the market opportunities and future potential of long-term utilization of cloud?

The aforementioned statistics related to costs associated with cloud and security practices and policy implementation, should be sufficient to convey the greater importance of cloud security in a corporate environment to both IT professionals, as well as the financial business executives.

While cloud migration is often favored, due to its cost-cutting and profit-revenue increasing nature, the organizations should not forget the risks and concerns that come along with it. Secure practice of cloud and regulation compliance with the policies, is as equally important as productivity improvement and ROI generation. It is better to keep the infrastructure safe and secure beforehand, rather than to pay a hefty amount of toll in compensation for the incident afterwards.

REFERENCES

[1]. Buyya, R., Broberg, J., & Goscinski, A. (2011). Cloud computing: Principles and paradigms. Wiley.

[2]. Rittinghouse, J. W., & Ransome, J. F. (2017). Cloud computing: Implementation, management, and security. CRC Press.

[3]. Whitepapers. (2020). Retrieved from https://docs.aws.amazon.com/whitepapers/latest/aws-overview/introduction.html

[4]. 2016-2021 Cisco Global Cloud Index: Forecast and Methodology. (2018). Retrieved from https://www.readkong.com/page/cisco-global-cloud-index-forecast-and-methodology-4248491

[5]. Hendre, A., & Joshi, K. P. (2015). A Semantic Approach to Cloud Security and Compliance. *2015 IEEE 8th International Conference on Cloud Computing*. doi:10.1109/cloud.2015.157

[6]. Zissis, D., &Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592. doi:10.1016/j.future.2010.12.006

[7]. Behl, A., & Behl, K. (2012). An analysis of cloud computing security issues. 2012 World Congress on Information and Communication Technologies. doi:10.1109/wict.2012.6409059

[8]. Union, C., & Parliament, E. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[9]. Owler, United Lex Competitors, Revenue and Employees - Owler Company Profile. Retrieved from https://www.owler.com/company/unitedlex

[10]. July 21, 2, Cyber Risk Solutions - UnitedLex Services. Retrieved from https://www.unitedlex.com/services

[11]. July 31, 2. UnitedLex Extends ISO 27001 Certification to Cover All North American Operations. Retrieved from https://www.unitedlex.com/news/unitedlex-extends-iso-27001-certification-cover-all-north

[12]. Managed SIEM, UnitedLex Services, Managed SIEM. Retrieved from https://bit.ly/2OmanQI

[13]. Unitedlex Corporation. A New Guide to Evaluating Managed Security Services Providers. Retrieved from http://info.unitedlex.com/rs/844-LCF-225/images/New-Guide-To-Evaluating.pdf

[14]. Unitedlex Corporation. Optimizing Litigation Life Cycle Management. Retrieved from http://info.unitedlex.com/rs/844-LCF-225/images/Optimizing%20Litigation%20Life%20Cycle%20Management.pdf

[15]. Unitedlex Corporation. Managed Detection and Response: How to Find the Right Partner for Your Organization. Retrieved from http://info.unitedlex.com/rs/844-LCF-225/images/MDR%20whitepaper.pdf

[16]. Rapid Response Platform,UnitedLex Services, Retrieved from https://bit.ly/2CD8Cs9

[17]. TAG Cyber (2018). 2018 TAG Cyber Security Annual, Volume 1: Outlook for Fifty Cyber Security Controls. Retrieved from https://www.tag-cyber.com/downloads/2018-TAG-Cyber-Security-Annual-Volume-3.pdf

[18]. Owler. IBM Competitors, Revenue and Employees - Owler Company Profile. Retrieved from https://www.owler.com/company/ibm

[19IBM, IBM Cloud Compliance Programs. Retrieved from https://www.ibm.com/cloud/compliance

[20]. IBM Whitepapers. Protecting Your Cloud: Maximize security in cloud-based solutions. Retrieved from https://bit.ly/33lcfzw

[21]. Murphy, J., & Wood, S. (2017). IBM Watson IoT Platform: Security and Risk Management - Presented at CRA IoT Summit. Retrieved from https://bit.ly/2DWh6LQ

[22]. IBM (2018). IBM Data Security and Privacy Principles - Service Level Agreement. Retrieved from https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW3/$file/Z126-7745-WW-3_05-2018_en_US.pdf

[23]. Paris-White, D. (2018). Five security services every cloud platform should provide. Retrieved from https://www.ibm.com/cloud/blog/five-fundamentals-cloud-security

[24]. Owler, Cloudflare Competitors, Revenue and Employees - Owler Company Profile. Retrieved from https://www.owler.com/company/cloudflare

[25]. Bos, E. (2017). Analyzing the Performance of Cloudflare's Anycast CDN, a ... Retrieved from https://pdfs.semanticscholar.org/a03a/c8898ef41ddefff69cbdab4acfdc04d6b291.pdf

[26]. Cloudflare (2020). Cloudflare Privacy Policy. Retrieved from https://www.cloudflare.com/privacypolicy/

[27]. Cloudflare, DDoS Protection with Cloudflare - Whitepaper. Retrieved from https://www.cloudflare.com/media/pdf/cloudflare-two-pager-ddos-protection-rate-limiting.pdf

[28]. Cloudflare, Securing Applications in the Cloud – Whitepaper. Retrieved from https://www.cloudflare.com/resources/assets/slt3lc6tev37/4ucRRiRjqFXViVMR6u62OO/ea79834b9e9858df6c226ed9943e4b98/cloudflare-securing-applications-cloud_Q42019.pdf

[29]. Cloudflare, a SaaS Provider Survival Guide: Cloudflare - Whitepaper. Retrieved from https://www.cloudflare.com/media/pdf/ssl-saas-white-paper.pdf

[30]. Cloudflare, Cloudflare for Enterprise - Whitepaper. Retrieved from https://www.cloudflare.com/resources/images/slt3lc6tev37/7jDID0lAuFxEM8MBcZHc0B/791393aa9eac3fc4e9c28d993d36924d/Cloudflare_Enterprise_Overview_2-pager.pdf

[31]. Lohstroh, M. (2018). Why the Equifax Breach Should Not Have Mattered. Retrieved from https://arxiv.org/pdf/1801.00129.pdf

[32]. Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. Business Horizons, 59(3), 257-266. doi:10.1016/j.bushor.2016.01.002

[33]. Sollars, M. (2016). Risk-based security: Staff can play the defining role in securing assets. Network Security, 2016(9), 9-12. doi:10.1016/s1353-4858(16)30087-3

[34]. Verizon's Acquisition of Yahoo: Deal or No Deal? - 8th Annual Brooks Case Competition. (2017). Retrieved from http://faculty.cbpa.drake.edu/suh/brooks/brooks-vz-yhoo.pdf

[35]. IBM & Ponemon Institute. (2018, July). 2018 Cost of a Data Breach Study: Global Overview. Retrieved from https://co-c.net/ressources/papers/2018_Global_Cost_of_a_Data_Breach_Report.pdf

[36]. Ferguson, S. (2016, September 29). Cloud Computing Embraced As Cost-Cutting Measure. Retrieved from https://www.informationweek.com/cloud/cloud-computing-embraced-as-cost-cutting-measure-/d/d-id/1327062

[37]. CompTIA (2016). Trends in Cloud Computing 2016. Retrieved from https://www.slideshare.net/comptia/trends-in-cloud-computing-2016

[38]. Cloud Endure (2017). Cloud Endure Cloud Migration Survey Report. Retrieved from https://www.coursehero.com/file/35548689/Cloud-Migration-Survey-General-SM-26-pagespdf/

[39]. Singla, A., Chandrasekaran, B., Godfrey, P. B., & Maggs, B. (2014). The Internet at the Speed of Light. Retrieved from https://www.cs.cmu.edu/~xia/resources/Documents/Singla_hotnets14.pdf

[40]. Persistent Systems (2016). Assessing The ROI Of Cloud An Executive Decision Framework - Whitepaper. Retrieved from https://www.semanticscholar.org/paper/Assessing-The-ROI-Of-Cloud-An-Executive-Decision/924ec0f54403af000a00ba22216abebfd997ea0d

[41]. Loadview by Dotcom-Monitor (2020). ROI Comparison: Cloud vs On-Premises Load Testing Tools. Retrieved from https://www.loadview-testing.com/learn/roi-comparison-cloud-vs-premise-load-testing-tools/

[42].
IBM, Ponemon Institute (Rep.). (2020). Retrieved 2020, from IBM; Ponemon Institute website: https://www.ibm.com/security/digital-assets/cost-data-breach-report/Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

[43]. Understanding Cloud ROI Factors (Research Paper). CITO Research.

How to cite this article: Das, P. and Kumar, N. (2020). Significance of Cloud Security Policies and Practices in Corporations and Organizations. *International Journal on Emerging Technologies, 11*(5): 320–329.