International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8009-8015

On Issues, Strategies and Solutions for Computer Security and Disaster Recovery in Online Start-ups

Omoruyi Osemwegie[1], Kennedy Okokpujie[2], Nsikan Nkordeh[3], Samuel John[4] and Adewale Adeyinka A.[5]

[1,2,3,4,5]Department of Electrical and Information Engineering, Covenant University, Ota, Ogun State, Nigeria.

[1]osemwegie.omoruyi@covenantuniversity.edu.ng, [2]kennedy.okokpujie@covenantuniversity.edu.ng, [3]nsikan.nkordeh@covenantuniversity.edu.ng, [4]samuel.john@covenantuniversity.edu.ng, [5]ade.adewale@covenantuniversity.edu.ng

Abstract

Vast majority of entrepreneurial ventures want an online and offline business model. Quite a good number would prefer their dealings occur strictly online. However, very few know what it takes to aim at achieving 99.999% availability, this is a key goal in deploying Computer and information technology (IT) solutions. In this present world of Information Technology there is an increase in threats faced by small medium businesses and enterprise on online platforms. More companies are vulnerable to attacks/threat such as DDOS, Malwares, Viruses, Ransomware etc. Entrepreneurial venture's adoption of IT solutions with security in view, in addition to a disaster avoidance, mitigation and recovery plan or strategy can help in this respect.

This paper suggests such issues to be considered and strategies to adopt in IT security and avoiding disaster and solutions to remedy disaster.

Keywords: Computer security, Recovery, Availability, Online Start up, Planning.

INTRODUCTION

A cursory look at major vendors of IT security solutions would suggest that most online start-ups and ventures are priced out of the IT security solutions market. Starting from discouraging statistics with regards to funding, IT start-ups especially in Africa are against huge odds for success from a financial perspective. Cost reduction therefore is key for IT start-ups. Majority of ventures consider the addition of IT Security and Disaster recovery (DR) solutions a luxury at best. Most will be hesitant in deploying IT solutions when compared to other cogent needs within their organizations. This means therefore that firms may not consider this a priority and may go without adoption of any comprehensive solution for IT security and disaster recovery. Hence increasing the chances of failure of their online business model which is what availability helps them avoid in the first place. Affordability of this solutions shouldn't stunt the Venture's growth neither should poor availability too. Decision makers (Entrepreneurs) need to be guided to understand the issues surrounding IT security and disaster recovery.

The study suggests that online ventures adopt best practices in deploying IT solutions especially to win their consumer confidence. Such custom based solutions can often times be evolved into a better comprehensive solution than market ready solutions. This study is broken down into the following, Section 2 is a review of relevant literature on goals of Computer security and then DR. Section 3 covers the important steps in the Disaster recovery planning i.e. drafting DR requirements, determining which DR strategies are most suitable, creating documentation and selection of backup solutions etc. Section 4 gives a number of strategies and examples from a broad range. Section 5 concludes this study.

REVIEW

IT Security or Computer security is defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications) [1]. In that sense, it has been identified that computer security aims to achieve specific goals.

i. Goals of Computer Security

1. Confidentiality ensures that computer-related assets are accessed only by authorized parties [2].
2. Integrity means that assets can be modified only by authorized parties or only in authorized ways [2]. It includes the integrity of system resources, information, and personnel [3].
3. Availability assures that systems work promptly and service is not denied to an authorized user [1]. Availability applies both to data and to services [2].

ii. Disaster Recovery planning

Disaster Recovery (DR) planning is a part of the computer security or business continuity plan that deals with coping after an event where there is a loss especially with regards to

data or computing infrastructure. DR Planning is an IT-focused plan that is designed to restore operability of the target systems, applications, or computer facility at an alternate site after an emergency [6]. Most DR planning are focused on the availability goal of computer security. However, the fact that significant data loss is involved after a majority of disaster for any organization makes the other two goals as well as other secondary goals like Authorization, Auditing and Authentication important in the DR process. The range of solutions for which DR planning covers include but is not limited to IT operations and system, production operations, workforce connectivity and infrastructure [11].

Geoffrey H. Wold proposed a ten point step process in DR planning that includes [7]:

1. Obtaining Top Management Commitment
2. Establishing a planning committee
3. Performing a risk assessment of the organisation with regards IT disaster.
4. Establishing priorities for processing and operations.
5. Determining the best recovery strategies to be adopted.
6. Performing data collection
7. Organizing and documenting of a written plan.
8. Developing testing criteria and procedures for plan.
9. Testing of the plan
10. Approval of the plan

iii. **Tiers of Disaster Recovery Solutions**

Disaster recovery solutions can be sub-classified using the TIER's approach as given by the SHARE group specification (1992) consisting of seven tiers as is visible from Figure 1. The approach sub-classes this different solution from a no-plan scheme to a completely lossless disaster recovery platform.

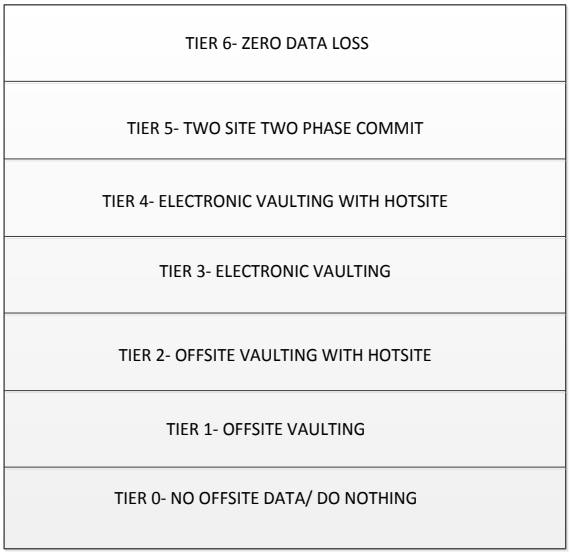

Figure 1: Disaster recovery TIER created from SHARE group specification created in 1992.

TIER 0 represents the base of solutions targeted at DR. At this level, little or no plan is adopted in resolving data or computing resource disaster. The organization goes about without an adopted plan or solution. TIER 1 is an offsite option or platform adopted as a disaster recovery plan or solution. Organization with traditional means of data storage may adopt this approach by keeping data backups in media devices or tapes, backup disk/ storages and have this physically transported to secluded or remote storage facilities. Such facilities could also be outsourced. Best practices suggests that organizations that offer this services be outside geographical location where its clients are based (say different Region or country). Similar geographic locations could mean that backups may be prone to same risk in offsite facility as in organization's facilities e.g. flooding earthquakes, fire outbreak, biochemical attacks etc.

TIER 2 provides an extra option of fast retrieval usually within days of disaster, organisation can retrieve most of what it lost by requesting from offsite storage facilities specified documents, tapes or backup media. TIER 3 includes electronic vaulting of data and other critical resources of the organisation. This would improve the rate of storage to offsite facilities by the inclusion of Wide area network facilities like the internet over which such business critical information can be transmitted. TIER 4 facilitates the process by which data can be recovered with ease from the Electronic vaulting platforms, say over the internet and provides quick access to business critical information. TIER 5 provides replica copies to all organizational data and information resource with high level bandwidth connections (fibre optic/satellite connections) often used. The TIER 6 represents an almost ideal layer with all parts of the business process totally electronic in nature and an almost instantaneous recovery process such that no data is lost.

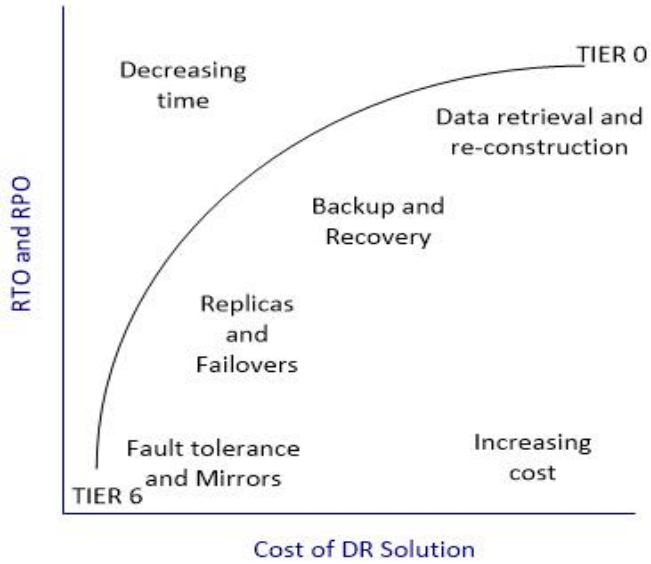

Figure 2: Showing relationship between cost of DR solution and Recovery Time Objective or Recovery Point Objective from the seven tier perspective.

While solutions have been developed for each tier, some tiers have become obsolete with respect to online businesses. The proliferation of Cloud based services and offerings mean that traditional cost models like that in Figure 1 are changing, however that does not make this chart obsolete. Costs for improved solutions for lesser tiers also declined. Decreasing costs for higher tiers solutions is made possible because of increased user base for cloud services which scales costs for services on cloud platforms.

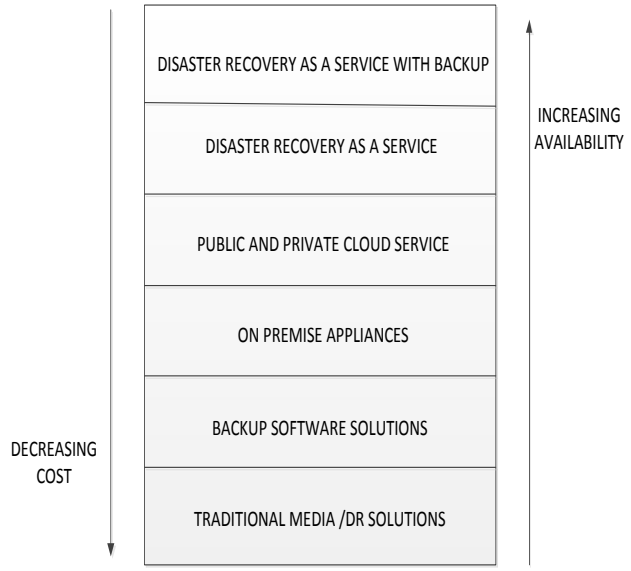

Figure 3: Cost model for DR solutions showing increasing availability with increasing costs. Although costs associated with cloud based services are spread over lifetime of use.

DR PLANNING FOR ONLINE START-UPS

Disaster recovery strategies can be classed with regards to type of measures taken into three:

a) Preventive

b) Detective

c) Corrective.

Also, DR solutions can be classed by its sources into two:

i. Vendor-specific

ii. Custom-built

DR solutions are a healthy mix of all three measures (preventive, detective and corrective measures). Custom-built solutions take into consideration not just the structure or needs of organizations but affordability of solutions. To draft custom based disaster recovery procedures one must have a clear cut understanding of the topology of Computer Network/IT solutions to be covered. Best practices mean that you can't afford to be reactive but be anticipatory and proactive to threats in setting up IT solutions or networks.

Failure or disaster may arise at any point within and without such solutions whether network, hardware or software. As all topologies may not be similar so also approaches to IT Disaster avoidance mitigation and recovery may not be the same. Drawing from [7] above start-up ventures are most times flat organizations with multiple roles assigned to specific individual. The chances of business failure are greatly increased with an outage in the business IT platform; especially for firms whose source of consumer interaction is wholly from an online basis.

The priority therefore would be to ensure that in the event of failure the Recovery Time Objective (RTO) and the Recovery Point Objectives (RPO) are kept reasonable. The former defines the time period after a disaster in which a business service will be restored, while the latter refers to the maximum time period in which data related to the business may be inaccessible after a disaster. RTO can also be defined as an orthogonal business decision that specifies a bound on how long it can take for an application to come back online after a failure occurs [13]. Anytime from say 6 hours and above for both objectives could considerably affect business activity. Whilst the RPO represents the point in time of the most recent backup prior to any failure [13].One useful step would be for online start-ups to evaluate through relevant analytical platforms the most probable time for user interaction or visits. For carrying out site analytics various platforms exist e.g. Google Analytics [8], Spring Metrics [9], Woopra [10] etc. When the start-up trades using a platform over which it has no control then it must seek to find similar tools to help understand site analytics from its platform managers/administrators. We propose a seven step planning process for DR for the form of business called the online start-up namely:

1. Setting up of DR planning team.

2. Definition of the network topology and risk posed.

3. Stating of DR requirements.

4. Determining the best recovery strategies to be adopted [7].

5. Testing and evaluation of the proposed strategy.

6. Organizing, documentation and adoption of a written plan.

7. Updating of the plan as the start-up grows.

I. Setting up of DR planning team

Start-ups are often times flat organisations with very few differentiation or hierarchy across the organisation. This means that all members of an organisation can also members of the disaster recovery team. The planning process involves various aspect of the organisation and therefore will require the commitment of its promoters or proprietors in achieving a seamless implementation also.

II. Definition of topology and network coverage and risk assessment

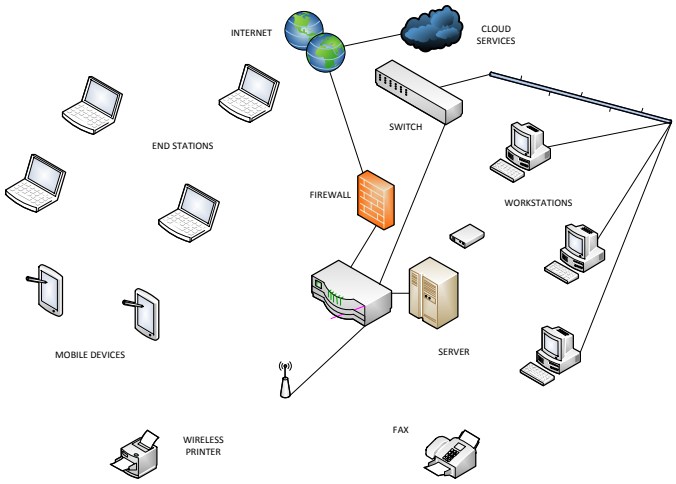

Figure 4: Typical Local Area Network

Network topology is at variance from organization to organization. As there is no one size fits all for network solutions so also there is no one size fits all for DR solutions. However DR solutions are dependent on the component parts of an organization's IT infrastructure. Whether from a Local area network or on from a Cloud perspective. The risk analysis to be carried out would cover the extent of the organisation's network topology. Risks in all aspects of the firm's IT operation should be identified and priorities be set as pertaining the levels of risk to be tolerated.

ii. Stating of the Disaster recovery Requirements

In developing DR requirements, certain questions are pertinent:

1. What is acceptable time to recovery? (RTO)
2. How much data/computing resource loss is acceptable? (RPO)
3. How much performance degradation is acceptable during a disaster?
4. For how long is any performance drop acceptable?
5. Can cost be saved on what is required to provide an alternative (for data and computing resources)?
6. What is the rate of data change for this alternative?
7. What is the difference in cost for this DR solution for the next year?
8. How much will we need to scale our solution?
9. How will clients access our systems/network/site in case of disaster?
10. Do we need to migrate IPs or can you use new ones? This may mean non-dependence on a singular platform for the business.
11. How often do we need to validate the DR site/platform (should in case DR solutions are cloud or PC based)? Do we test every quarter, 6 months or once a year? With respect to an outsourced platform this may not hold but this information can be sourced through platform administrators.
12. When does the DR solution need to be in place?
13. How much of a downtime will be acceptable for returning back to the main site or facility? How much in advance do we need to schedule it?
14. Who decides that it is now a disaster and failover to alternate site (or backups) should occur? What are the criteria for the decision?

IV. Determining the best recovery strategies to be adopted

Issues and Strategies to be considered differ depending on network topology and risk exposure. Below are a few areas that are most ties critical to the business:

a. What do I do should a data centre or ISP service be disrupted?

Am I over-dependent on a singular ISP? How do I provide redundancy on this link? Fibre optic and satellite-link or fibre optic vs satellite link, Broadband or Public Wi-Fi. What Broadband service speed is preferable? What cost am I willing to incur on the fall back solution?

b. Web Hosting Solutions

Cloud hosting: Hosting solutions accessed over a Cloud service platform. Example Amazon AWS, Microsoft Azure, Google cloud etc.

On-site hosting: Hosting solutions custom built to organisation's needs using diverse vendor software and hardware.

c. Has the webserver crashed? This could be a Failure of the webserver system process, a DOS Attack, or a Failure of the web application.

System process failure

This can be resolved by stopping and restarting IIS, Apache system process etc.

Scalability and DOS Attacks: How do we design a more scaled application if this failure is due to increased user numbers on the site? Why didn't we adopt the use of CDNs before now?

d. Failure or attack of the Web-server/other auxiliary servers (mail, database etc.)

Failure of web application:

What do our custom error logs and web-server logs say about the matter? Can we debug quickly to resolve challenge? If we can how quickly? Can we put up a maintenance page while that is done? Or can we redirect users to other parts of the application that still works?

Has the physical server failed or crashed? If so then what caused it? Do our cloud or analytics server give us a clue? How quickly can we restart the server? Will this challenge reoccur?

Ways of configuring a site's Domain name

What type of Record does the website work with?

Alias-Record or A-record: An A record maps a domain, such as contoso.com or www.contoso.com, or a wildcard domain such as *.contoso.com, to an IP address. So the main benefit of an A record over a CNAME record is that you can have one entry that uses a wildcard, such as *.contoso.com, which would handle requests for multiple sub-domains such as mail.contoso.com, login.contoso.com, or www.contoso.com [20].

CNAME-Record: A CNAME record maps a specific domain, such as contoso.com or www.contoso.com, to a canonical domain name. In this case, the canonical domain name is the [myapp].cloudapp.net domain name of your cloud hosted application. Once created, the CNAME creates an alias for the [myapp].cloudapp.net. The CNAME entry will resolve to the IP address of your [myapp].cloudapp.net service automatically, so if the IP address of the cloud service changes, you do not have to take any action [20].

Failure of Web-server

With A-record, you may need blocks of IPs' as a strategy for disaster recovery. With CNAME Records, you can implement a redirect to another named server when there's a failure. All of this should be factored in with attention to costs both pre-disaster or failure and post-disaster and failure. E.g. a web company with 30 users would have different ideas compared to another with 30 million users.

Database server failure

To undertake recovery of database if there's a failure you need to understand two concepts:

Sharding or Partitioning: It is the process of splitting your data into multiple database instances, so that every instance will only contain a subset of your data. E.g. Images can be split based on month of registration, profile name etc. and placed in separate instances.

- It allows for much larger databases, using the sum of the memory/disk space of many computers. Without partitioning you are limited to the amount of memory/disk space a single computer can support.

- It allows scaling the computational power to multiple cores and multiple computers, and the network bandwidth to multiple computers and network adapters. See [19].

Data Replication: Data replication is a very simple concept. Replication can be configured in various modes namely:

- Master-master allows other master database servers to be exact copies of a key master server. The extra advantage being that the other master database can be used directly.

- Master-slave replication that allows slave database servers to be exact copies of master servers. Slave database servers can not be used directly. They are referred to when master databases fail to respond.

You must decide as a database administrator to adopt any of this two strategies to varying degrees in the event of a failure in the Database. Sharding can be adopted when database spaces are quickly exhausted while replication in the case of accidental or criminal wiping out of data.

*Backup***:** SQL databases can be scheduled to back up at intervals.

Mail server failure

Is my mail server solution bundled with my web application or separate? Is it outsourced or derived from a third-party provider or deployed on the organization's internal network. How quickly can this service be resolved in any of this cases? What's the loss to my organization if a mail is undelivered (factor all scenarios)? How much can be expended to adopt any of this solutions?

e. Failure of work stations and other devices

Here flexibility as to what approach can be adopted to ensure that organizational downtime is avoided. Multiple routers can be deployed; Users on one router can be switched to another should there be a fault with a router. An access point (AP) can be reconfigured or deployed quickly when wireless users are yanked off due to failure of an AP device in the network. Work stations can be repaired and replacements sourced, backup to disk (or SANs) etc.

f. Software/Web development solution failure

What occurs if web collaborative software or web development solutions fail or its related data are lost? What strategies are in place?

- Subversion (AnkhSVN, VisualSVN etc.)

- Repositories

- Backup servers or disk

- Gits

Solutions shouldn't be lost because a team member is unavailable. Cloud solutions can also be considered.

g. Failure of Primary power solution

Public power supply in most parts of Africa are often erratic and unavailable. Backup power solutions are relevant to enable availability especially for continuity in operations. Cloud data centres typically have much more robust solutions.

h. Obfuscation and Data encryption Techniques

Source code obfuscation is widely used to prevent/limit malicious attacks to software systems conducted by decompiling and understanding or modifying source code [14]. Software or web based applications may need to be kept confidential especially to only authorized personnel. The ability to reverse engineer such executables can create opportunities for theft of intellectual property via software piracy, as well as security breaches by allowing attackers to discover vulnerabilities in an application [15].

FURTHER DISCUSSIONS

Access control

Access control refer to issues concerning access of system resources and there are two primary parts to access control, namely, authentication and authorization [4].

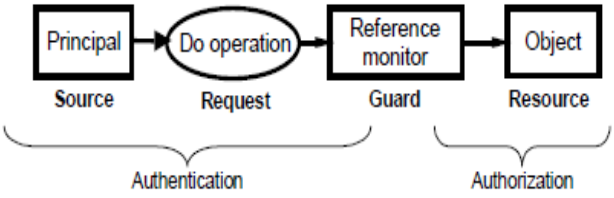

Figure 5: Access control Model [17]

Authentication

The authenticity property is a property of being genuine and being able to be verified and trusted; it is the confidence in the validity of a transmission, a message, or message originator [1]. Authentication ensures. X.800 [18] defines two types of authentication namely: data origin authentication, and peer entity authentication. The former refers to the corroboration that the source of data received is as claimed and the latter refers to the corroboration that a peer entity in an association is the one claimed [18]. In implementation, the use of Multi-factor Authentication is popular, having the advantage of improving the strength of Authentication. Passwords are usually the objects where they are most applied to.

Authorization

The granting of rights, which includes the granting of access based on access rights; this rights are the rights to perform some activity (such as to access data); and that they have been granted to some entity, human agent, or process [18]. Access rights are granted based on stated security policies.

Analytics

Web analytics is a process through which statistics about website use are gathered and compiled electronically [16]. Unlike Intelligence, Analytics investigates the reasons for user behaviour on a web site. They are a great tool for online start-ups because they provide valuable insight to frequently used features. This provides help in DR planning for setting priorities.

CONCLUSION

Web technology in the Web 2.0 era, certainly poses several uncertainties for new entrepreneurs therefore need for adequate knowledge covering old and new aspects of a web business cannot be over emphasized. However, such knowledge must be structured in a tangible. The goal of this study is to provide entrepreneurs with such a tool to cover this aspects.

ACKNOWLEDGEMENT

We acknowledge the support of Covenant University in conducting this research and the cost of publication.

FUTURE WORK

Future plans are to apply related studies in Disaster recovery (DR) to the Covenant University Ruckus Enterprise Wireless Network. This network supports roughly 10,000 persons.

REFERENCE

[1] W. Stallings, Cryptography and network security, 1st ed. Upper Saddle River: Prentice Hall, 2014.

[2] C. Pfleeger, S. Pfleeger and J. Margulies, Security in computing, 4th ed.: Prentice Hall Professional Technical Reference, 2002.

[3] J. Kizza, Computer network security, 1st ed. New York: Springer, 2005.

[4] M. Stamp, Information security, 1st ed. Hoboken, N.J.: Wiley, 2013.

[5] G. Wold, "Disaster Recovery Planning Process Part 2 of 3", https://www.drj.com, 2017. [Online]. Available:

http://www.drj.com/drj-world-archives/general-dr-planning/disaster-recovery-planning-process-part-2-of-3.html. [Accessed: 22- Feb- 2017].

[6] Disaster recovery strategies with Tivoli storage management, 1st ed. [San Jose, Calif: IBM Corp., International Technical Support Organization], 2002.

[7] G. Wold, "Disaster Recovery Planning Process Part 1 of 3", https://www.drj.com, 2017. [Online]. Available: http://www.drj.com/drj-world-archives/general-dr-planning/disaster-recovery-planning-process-part-1-of-3.html. [Accessed: 22- Feb- 2017].

[8] "Google Analytics", analytics.google.com, 2017. [Online]. Available: https://analytics.google.com/. [Accessed: 26- Mar- 2017].

[9] "Home", Spring Engage, 2017. [Online]. Available: http://www.springmetrics.com/. [Accessed: 26- Mar- 2017].

[10] "Real-time Customer Analytics - Woopra", Woopra, 2017. [Online]. Available: https://www.woopra.com/. [Accessed: 26- Mar- 2017].

[11] M. Jameson, "How to Develop an Effective IT Disaster Recovery Plan", http://www.drj.com/webinars/on-demand/september-7-2016-how-to-develop-an-effective-it-disaster-recovery-plan.html, 2016.

[12] G. Wold, "Disaster Recovery Planning Process Part 3 of 3", https://www.drj.com, 2017. [Online]. Available: http://www.drj.com/drj-world-archives/general-dr-planning/disaster-recovery-planning-process-part-3-of-3.html. [Accessed: 22- Feb- 2017].

[13] T. Wood, E. Cecchet, K. Ramakrishnany, P. Shenoy, J. van der Merwey and A. Venkataramani, "Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges", in HotCloud, 2010, pp. 8-15.

[14] P. Tonella, M. Torchiano, F. Ricca, P. Falcarin, J. Nagra, M. Di Penta and M. Ceccato, "Towards experimental evaluation of code obfuscation techniques", in 4th ACM workshop on Quality of protection, 2008, pp. 39-46.

[15] C. Schulze and A. Balakrishnan, "Code Obfuscation Literature Survey", CS701, 2005.

[16] S. Peltsverger and G. Zheng, "Web Analytics Overview", In Encyclopaedia of Information Science and Technology. IGI Global, pp. 7674-7683, 2015.

[17] B. Lampson, "Computer security in the real world", Computer, vol. 37, no. 6, pp. 37-46, 2004.

[18] The International Telegraph and Telephone Consultative Committee Recommendation, X.800: Security architecture for Open Systems Interconnection for CCITT applications, 1st ed. International Telecommunication Union, 1991.

[19] "Redis", Redis.io, 2017. [Online]. Available: http://redis.io. [Accessed: 26- Mar- 2017].

[20] "Configure a custom domain name in Cloud Services", Docs.microsoft.com, 2017. [Online]. Available: https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-custom-domain-name. [Accessed: 26- Mar- 2017].