Best Practices for Information Security in an Organization

[1] **Shaikh Juveria Shahnawaz, [2]Prof. Shailaja Gogate**
[1,2] Information Technology (Info. Security), Mumbai University,
Vidyavihar East, Mumbai, India
juvairia06@gmail.com

Abstract— **Information is the core of any organization, misuse of information can lead to destruction of an organization but still every organization is not fully aware of the losses that could be caused because of the loss of information. Many organizations do not have information security in their critical area where the losses can takes place. And on the other hand security breaches takes place day to day and to recover the breaches is very expensive. Here in this document I have come to some topic which will cover the information security policy. I have design best practices of information security in the critical area for every organization, so that if they will follow the below practices it will beneficial for their information security management system.**

Index terms- **Information security, access-control, server and network monitoring, cyber security, data center security.**

I. Introduction

Information security is the practicing to protect the information from security breaches, attacks, disclosure, use, unauthorized access, destruction, examining which is usually in the form of data takes place in electronic system (i.e. computer).

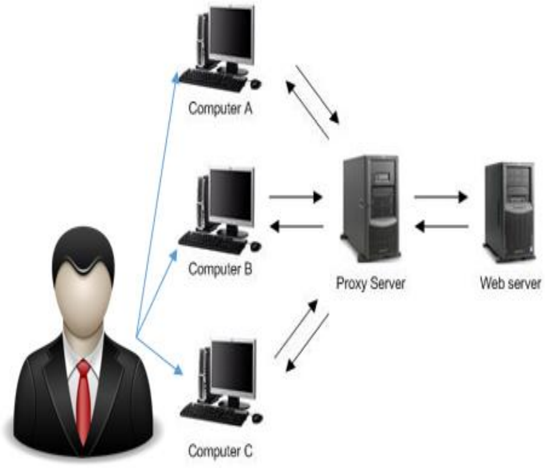
Every organization has their own information security policies and they follow their own and the organizations who are ISO/IEC 27001:2013 certified they follow ISO/IEC 27001:2013 open standards which are mandatory for the organization being ISO/IEC certified.

Traditionally, organization has their security documented policies in which the regulatory requirement covered the most, which may be true for building a strong information security program but that was for past. As from now with the development of the technology one should have good information security.

Strong policies to be build information security program for business perspective which in turns help to keep the customers who works for organization and to get in to new ones by attracting them by keeping the priority of information security policies on the top.

But it is not necessary for every organization to have the best security policies like area covers in ISO/IEC 27001:2013. But the best practices which I will covers some area will help at some extent to keep secure information from breaches, disclosure or anything else which in turns can cause loss for an organization.

It is very important for an organization that their technology, procedure, and policy to be secure for getting a business to higher extent. Documented policy would work excellently if this policy would be trained to the existing employee, because no one likes to read the policy manual. The only important thing is the company should at least follow this best practices or something from best practices who all are not ISO/IEC 27001:2013 certified.



II. IMPLEMENTATION

A. Access control

1) Create a baseline for access:

It’s the initial part of any IT department. Generate a baseline of current access level, by having records from different department of IT and control in that place. By this the organization can see gap in their current processes and can quickly catch a large offender. Baseline for access is generated according to the user needs and requirement for their use. So it is important to know the users need access for different functionality.

2) Automate user provisioning

Organization should monitor the sign in – sign out process or any inappropriate activity by user.

3) Tie Access control to organization environment

Here the access control should take place according to the working environment of an organization as different organization has different regulation. To what extent the user should have access to an organization depends upon the work environment of an organization.

4) Separate access using roles.

According to SOX, all among other regulation, demands separation of duties: the people who have right to approve the transaction shouldn't be allowed to access that account payable application, and the developers shouldn't have direct access to the financial data in the production system.

5) Monitoring unusual activity

It is important to monitor the user activity because if the user forgets the password then the person who is monitoring the activity will help in recovery.

B. Server and Network monitoring

1) Core monitoring

The organization should be sure about the core monitoring configured for all of their systems. CPU usage, drive space, memory usage and bandwidth should be collected for the servers. The bandwidth level on each interface is collected for switches and routers with SNMP monitoring over it. By having 24*7 core monitoring which will give clear views of system performance that allows the organization to detect potential issues.

2) Profile based Configuration

Different system have individual role according to employee profile but group of the system shared some properties too. The authentication for employee should be created according to their profile and should be monitored by the administrator of server. If the credentials are changed then it should be updated on server and the administrator could easily know about the changes.

3) Notification profiles

There are the different classes of alert and the most critical alerts are login events which is informational alert, low disk issues which are warnings alert, and finally the third is critical alerts for when vital systems are down. This three are the most critical alerts and it should be define properly before assigning them. If the change is needed in the profile of alert the only modification is need and all monitoring actions will pick up the change automatically.

4) Visual Displays

Dashboard should build in such a way that the status of critical IT systems should be shown. Build default dashboards that come with software and customize them by resizing existing elements adding new ones and by designing network diagrams. Display the network monitoring status so that employee should know the status of network operations.

5) Regular reports

Generate the reports of IT issues of network and server of particular system and deliver them to the individual employee for different customer, so that the will be are of the issues which takes place.

C. Cyber security

Application based data access should always be monitored as data are very sensitive and it can put business at risk.

Detailed logs and report data of IT activities should be collected should for both troubleshooting and security purposes. It's especially for a case where internal logging that doesn't have internal logging. This can be done by adding tools which create and report detailed logs.

Regular patches which are released on every second Wednesday of a month should be applied in IT infrastructure. It should be tested before applying. Patches should be maintain as cyber criminals are constantly inventing new techniques and always looking for new vulnerabilities, an optimized security network is only optimized for a long time.

Beware of social engineering because usually hacker tries to hack data from social engineering. It's better to block such social networking sites.

Users should be trained how to secure their information. The training should consist of how to recognize a phishing email, to create strong passwords, avoiding dangerous applications, taking information out of the company, and any other relevant user security risks.

Always monitor user activities, no matter they are trustworthy but verification is the duty for information security. Check whether they following best practices of cyber activity for keeping information to be secure.

How well you follow these best practices, you might get breached and in fact many organizations suffered security incidents in the past year. If the organization have the response plan it may allow to close vulnerabilities and limit the damage the breach can do.

D. Data center.

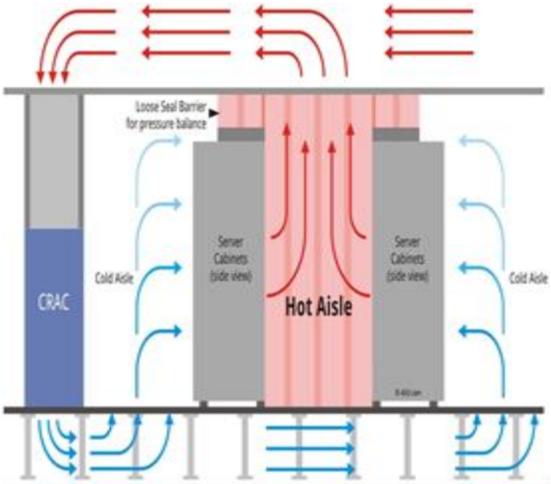


Fig. No 2

1) Maintaining air conditioning loops which comprising and supply air. Maximize the return temperature at the cooling units to improve capacity and efficiency of the data center.

2) The most efficient cooling system is that matches needs to requirements and matches of cooling capacity airflow

with IT loads. This prove to be a challenge in the data center as cooling units are sized for peak demand, which rarely occurs in most of applications.

3) Focus on cooling should be more which will reduce to consume energy and that can be done by increasing of fan efficiency, enhancing heat transfer, incorporating economizer.

III. BENEFITS

- If an IT organization follows this best practices it will reduce the security breaches.
- This will make information to be secure by having secure environment of these best practices.
- This will increase the trust on client that the organization focus on information security and will increase profits by increase in clients.

IV. CHALLENEGES

- This can be expensive to follow this over all best practices for small and initial start-up companies.
- For overall best practices, organization likes small start-up they cannot follow overall except some of these.

CONCLUSION

The organization of small core, if they follow best practices which I have mentioned then organization will surely reached to an extent level of information security.

These best practices are not only for IT companies but this can also be used for non IT companies where the use of data center, internet access, is there.

ACKNOWLEDGEMENT

I have taken efforts in writing this report. However, it would not have been possible without the sheer guidance and constant support of many individuals. I would like to extend my thankfulness to all of them.

I would like to extend my deepest gratitude to Prof. Shailaja Gogate, Associate professor of K.J.S.C.E in department of Information Technology, for providing me the opportunity in writing this paper. She has been very supportive in offering constant guidance in every milestone achieved during my paper publishes tenure.

I would like to thank Mr. Amjad Shaikh, Corporate Info Sec & Risk Group, L&T Infotech Pvt. Ltd. For giving me an idea related to publish paper.

Last but not the least; I would like to thank my family and friends for motivating me all the time.

References

[1] http://corporatecomplianceinsights.com/information-security-best-practices/ by Matt Putvinski,

[2] http://www.frameflow.com/five-best-practices-for-network-and-server-monitoring/ by frame flow

[3] http://www.observeit.com/blog/10-best-practices-cyber-security-2016 ObserveIT by Matt Zanderigo.

[4] The Enterprise Data Center Design Guide by white paper experts in business continuity.

[5] https://en.wikipedia.org/wiki/ISO/IEC_27001:2013.

[6] http://www.iso.org/iso/iso27001.

[7] http://www.itgovernance.co.uk/what-is-cybersecurity.aspx.