Importance of Information Availability, its effects on Business & the proposed Model

* Bilal Alvi ** M. Wasim Qureshi and *** Shakir Karim

***Abstract*—Many a time the irony one can face is the unavailability of the resources when they are needed the most causing unavoidable/irreversible loss. These kinds of scenarios can cost organizations their business. Enterprises suffered and are still suffering a huge loss in terms of revenue, customers' dissatisfaction and more. Though availability is one of the three basic components of security besides Confidentiality and Integrity, it could not get its due share and remained under the back- drop. In this paper, the importance of the information availability and its key determinants are discussed, analyzed and a conceptual model is proposed. The model is validated by carrying out an in-depth study of three major multinational oil enterprises of Pakistan. The study proved that if information availability is taken care in true sense, success in business could be assured.**

Received: June, 25, 2008, Accepted: July 17, 2008

***Index Terms*—Accessibility, Information availability, Information security, Reliability.**

I. INTRODUCTION

The information availability is as important a security factor as the confidentiality and integrity, however it can't be overemphasized. For any business to grow successfully the information availability plays a vital role leading to continuous uptime and minimum downtime, which is the mission of every successful business organization [1]. With the advent of information technology (IT) almost 100% successful businesses of the world have gone hi-tech with respect to hardware and software, requiring all the ingredients of IT; the list for which is quite an exhaustive one – from advanced Servers to simple Applications. Organizations should be able to access data without any interruptions to compete and stay in the market and business [2]. The term comes to mine that help summing up the above discussion is "information system" that describes the systematic collection, processing, transmission and dissemination of information with respect to very well defined procedures that may be manual or in most of the cases automated.

The world of IT is not a bed of roses as it seems, there may be all kinds of threats may it be virus, hacking, spoofing or any other form waiting to play havoc with any organization from minor damage to complete wipe out of the stored data.

In the above-mentioned context – mission, objective and goals of any organization are very critical that provides the guidelines in making the information available. Therefore it may be suffice to say that availability of information has hand and glove relationship with security. But whilst there are numerous formal models for confidentiality and integrity, there is no model for availability that would define the concept with rigor [3]. It can be safely assumed that by raising the level of security, may it be physical or logical; percentage of availability of information with respect to time can be drastically enhanced. It may not be enhanced to the level where its availability to desired personnel may cause delay due to unnecessary checks. So it is quite clear that importance of security cannot be overlooked and we should remain cognizant of the fact that it must be cost effective. As it is said that the safest node, on the widespread Internet with hackers and crackers in hunting mood, is the one is the one that is switched off – which is definitely **not** the solution.

The aim of this paper is to analyze how to address the factors of availability in organizations and thereby identifying the key determinants (attributes) of information availability by carrying out an in-depth study of organizations. The same would help in developing a broad based model.

II. HISTORY AND BACKGROUND

Confidentiality, Integrity and Availability – the three pillars, have been identified as the key components of the information security. However, only confidentiality and integrity remained in the limelight in the past one of the reasons may be leaking of the information to foes to any business, may it be corporate sector or any other organization [4]. The importance of downtime was never realized and was always taken as afterthought. Numerous models for confidentiality and integrity may be found but no such model for availability can be traced and it remains in the backdrop. It is the high time to realize that one of the aims of an attacker is to make the system unavailable thereby causing quite an unavoidable loss, which can be evident by table I [5] that provides a brief overview of major incidents due to which system remained unavailable over the past few years.

It would be of utmost importance to discuss as to what constitutes information system? and what information security is?

* *Department of Electronic Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan.* alvibilal@hotmail.com

** *Pakistan Petroleum Limited (PPL)*

*** *Department of Electronic Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan.* mailtoshakir@gmail.com

Table I- Major Information security incidences

Name	Impact
Morris Worm	Stopped 10% of computers that were connected to the Internet.
Melissa Worm	100,000 computers infected in one week causing $1.5 billion loss
Explorer Virus	$1.1 billion loss
Love Bug Virus	$8.75 billion Loss
Sircam Virus	2.3 billion computer infected causing $1.25 billion loss
Code Red Worm	359,000 computer infected in <14 hours causing $2. 75 billion loss
Nimda Worm	160,000 computer infected causing $1.5 billion loss
Klez	$750 million loss
BugBear	$500 million loss
Badtrands	90% of vulnerable hosts infected in just 10 minutes, $400 million loss
Sapphire/Slammer worm	75,000 hosts infected causing $1.5 billion
Blaster	$750 million
Nachi	$500 million
SoBigF	Fastest spreading mass-mailer worm causing $2.5 billion loss
MyDoom Worm	More then $4.0 billion loss due to 100,000 instances of the worm/hour
Witty Worm	First wide-spread worm to carry destructive payload

Information system means any node that is helpful in transferring information. It may be computers, communication facilities and Networks that help to move data or information to and fro including programs, specifications, and procedures, operations, use and maintenance.

III. INFORMATION SECURITY

Information security encompasses the measures for prevention, detection and recovery of the data. In addition, it includes measures regarding education, awareness and training required to support the protection of information assets [6]. The major among all is the information availability that has to be taken into account. The literal meaning of ‘availability’ is “able or ready to be obtained or used”. It is a measure of time duration when the system under consideration not only remains up without any outages but also performs the desired function efficiently and optimally and remain accessible to its desired users and its deprived are not deprived to the authorized users.

It is observed that availability, whenever considered, realized as an after-thought, as it is generally talked with reference to National Disaster or some Untoward Incidents that may make system unavailable. In fact availability should be discussed with every aspect that may hinder a user to access the system and makes it unavailable leading to defining a Policy, Each threat, whether it be a virus threat or some other kind of malicious act, must be the part of the security policy. Availability unlike its counterpart, confidentiality & integrity, cannot ensure by preventing illicit access to information within computer system.

The fact is not as simple as it seems to be, Availability is directly related to both information as well as resources. Keeping in mind the above, threat against availability may be categorized as

- Excessive workload on the server that hampers the timely provision of services to its client.
- Malfunctioning of the system due to some physical failure such as Hard Disk goes down.
- Poorly administered and configured system.

The above discussion infers that confidentiality and integrity can be achieved with a high level of enforcement but the same may not be true for the availability [7].

Computers have revolutionized all walks of life including industries, which have become information intensive and require it’s timely access to carry out routine work. Employees are getting comfortable and more used to computers carrying out transactions over the Internet. It is rightly said that we are marching towards ubiquitous computing [8]. However, heavy dependency on IT has paved the way of numerous attacks that may result in significant losses, threats and damages to the enterprise. Threats may be accidental or deliberate (human or device) but they all lead to common path – Unavailability, Threats exploitation of vulnerabilities, caused due to inherent flaw in the physical environment/procedures is a continuous chain. Most of the vulnerabilities are the cause of loopholes in security controls. It may be incorrectly configured or not updated [9]. It may come in any shape or size, from national disaster to random/accidental system faults [3]. It may be the Denial of Service (DoS) or Distributed DoS.

IV. METRICS REGARDING INFORMATION AVAILABILITY

The importance of information availability, as discussed earlier, raises questions as how not to over emphasize the level of availability, who will decide what level is to achieve regarding availability of information and how to ensure the maximum availability? These all include making the system redundant, providing system backup, designing pro-active policies etc. There must be some kind of metric associated with the availability. Researchers generally do it in terms of Latency [3], Mean Time to Fail (MTTF) and Mean Time to Repair (MTTR) [10], also called as Mean Time to Restore & Mean Time Between Failure (MTBF). All these measure the amount of time an information source was unavailable but from a different perspective. MTBF and MTTR are the most commonly used metrics [11]. MTBF measures average amount of time between failures, on the other hand MTTR measures average time required to repair/restore a failed system.

Availability may be measured, as the ratio of the time a system remains available to the time it should have been available. Ratio is calculated using both MTBF and MTTR

$$Availability = MTBF / (MTBF + MTTR)$$

where,
MTBF = Mean Time Between Failure
MTTR = Mean Time to Repair

From above-mentioned formula it is evident that by keeping MTBF greater than MTTR we can achieve an healthy percentage of availability. In complex world of networks, which plays a very crucial role, it is of utmost importance that all the components are combined in parallel rather than in series for higher system availability [12]. This shows *Availability* depends upon reliability and downtime of a system. Following is discussed how to quantify these two factors.

V. MEASURING RELIABILITY

Reliability can also be measured as the failure rate; it is inverse of either hardware MTBF or system MTBF. Mathematically it can be writtern as

Failure Rate = 1 / MTBF

where,

MTBF = Mean Time Between Failure

MTBF and Failure Rate change during the operational life of a component as High – to – Low – to – High curve, also called as the Bathtub curve [13] for its resemblance with the shape of bathtub. The curve is depicted in figure 1.

It is pertinent to mention here that MTBF may not be confused with component's useful life, as they are not interrelated. For example, a component may have a useful life of four hours and have MTBF of 100,000 hours [13].

VI. DOWNTIME: PLANNED & UNPLANNED

Downtime, regarding availability of information, can be discussed as planned and unplanned.

Planned downtime occurs when a system must be made unavailable for maintenance, repair, upgrade or any other planned event, whereas unplanned downtime results from failure [11]. Implementing proper testing, configuration and monitoring methodology Unplanned downtime can be reduced [11]. A service level agreement (SLA) between vendor and the concerned company can help minimizing MTTR. To achieve highest degree of availability, the proposition should be the amount of time the system would be available for productive use.

Each organization has its own availability target in accordance with its objectives, mission and goals, for instance, table II [5] provides a ready reference of different availability targets, which can be achieved with its respective downtimes.

In real life, getting near to 5 and 6 nines [14] would be a real achievement, which requires excellent planning, professional administration, real time tested standards, operating procedures, well trained staff and probability of little luck [13].

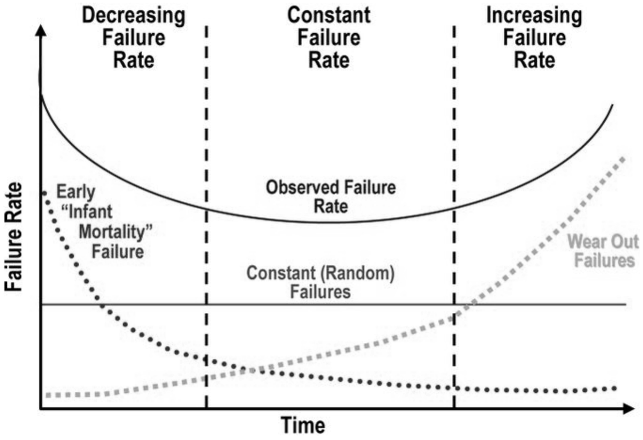

Fig. 1 Component Failure Rate Bathtub Curve

Table II - Availability targets with respective downtimes

Nines	Availability Target	Downtime/Month	Downtime/Year
	95%	36.0 hours	432.0 hours (18 days)
	97%	12.6 hours	259.2 hours (10.8 days)
	98%	14.4 hours	172.8 hours (7.2 days)
2 nines	99%	7.2 hours	86.4 hours (3.65 days)
3 nines	99.9%	43 minutes	8.6 hours
4 nines	99.99%	4.3 minutes	52.26 minutes
5 nines	99.999%	26 seconds	5.256 minutes
6 nines	99.9999%	2.6 seconds	31.1seconds

The importance of downtime has lately been realized. Number of service providers, competing against each other, proves their worth in the eyes of the customers with a gift of minimum downtime. This suggests that downtime can directly be related to loss of revenues, additionally, it may ruin organization reputation; spoil relationships with customers, suppliers and business partners [11]. The cost associated with the downtime could be in terms of

- Hard Costs
  Hardware/Software, IT staff time and
  Resources required remedying an outage situation
- Semi-Hard Cost
  Business lost during outage
- Soft Cost
  Loosing public confidence and/or business opportunities

Cost versus Benefit is represented in figure 2. The expense cost differential (ECd) is the difference between the investment to achieve a certain degree of availability and what system's downtime is calculated to cost the business [2].

VII. KEY DETERMINANTS OF INFORMATION AVAILABILITY

During the course of research, following attributes were identified as the key determinants of information availability. The detail is self-explanatory.

- Physical and Logical security
- Information security policy
- Operational control processes
- Pro-active hardware management
- Hot spares' inventory
- Tested and certified configuration
- Load balancing and configuration management
- Continuous system monitoring and inspection
- IT auditing and system effectiveness evaluation
- Hardware redundancy

- Data backup
- Business continuity

Each key determinant has an important role to play, however, it is the security policy that harnesses each aspect and dictates as to how the IT infrastructure would be implemented, operated, maintained and, when necessary, terminated. It sets the foundations for successful enterprise operations.

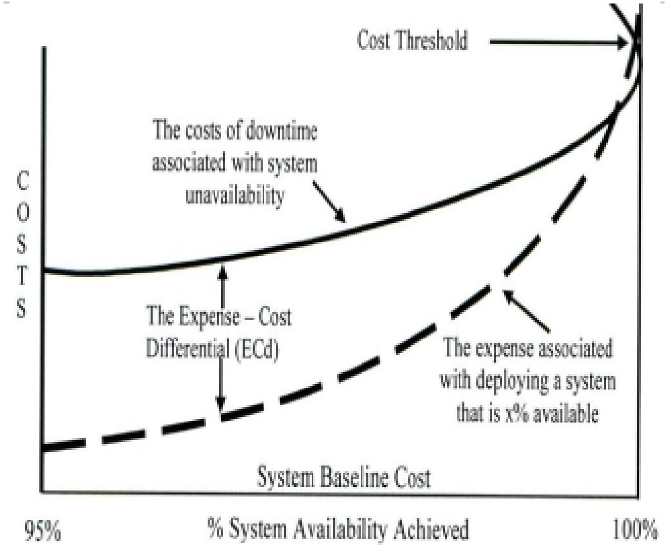

Fig. 2 Cost Vs Benefit Curve of Availability

Availability can be subdivided into three components, namely, Reliability (R), Accessibility (A) & Timeliness (T) as depicted in figure 3.

Each determinant affects one or more of these components, thereby, has a profound impact on information availability.

VIII. PROPOSED MODEL OF INFORMATION AVAILABILITY

It may be difficult to propose a model that fits in on all the organization; however, it is very much possible to propose a broad based model that includes all the key determinants.

The determinants are defined in the subgroups mentioned by the intersections in fig. 3. The key determinants “IT auditing & System effectiveness evaluation “will affect Reliability and Timeliness. “Proactive hardware management, Load balancing, Data backup & Business continuity” drives the status of Availability and Timeliness. The driver determinant for Reliability and Availability is “Physical and Logical security”. The determinants affecting all the three components are Information security policy, Operational control processes, tested and certified configuration, Continuous system monitoring and inspection, and Hardware redundancy.

Organizations may adopt it in totality or choose a number of them to implement those in their organization according to their goals, aims, objectives and business needs. It will also help the organizations in defining policies more objectively. It was analyzed that if an organization addresses each of these determinants, the availability of information can easily be ensured.

IX. VALIDATION OF PROPOSED MODEL

To check the efficacy of the proposed model, three Enterprises were short-listed to carry out an in-depth study and analysis. The said enterprises belonged to varying environments, both national and multinational inclusive.

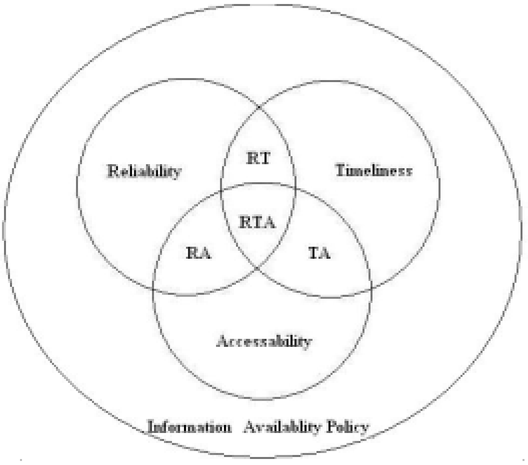

Fig. 3 Proposed model of Information Availability

Table III [5] shows the Key determinants adopted and implemented.

Table III - Key determinants in proposed model Vs existing model

Key Determinants	Proposed Model	Enterprise-I Existing Model	Enterprise-II Existing Model	Enterprise-III Existing Model
Physical & Logical Security	Yes	Yes	Yes	Yes
Information Security Policy	Yes	Yes	Yes	Yes
Operational Controls processes	Yes	No	No	No
Pro-active Hardware Management	Yes	No	No	No
Hot Spares’ Inventory	Yes	No	No	No
Tested & Certified Configurations	Yes	Yes	No	No
Continuous System Monitoring & Inspection	Yes	No	No	No
Load Balancing & Traffic Management	Yes	No	No	No
IT Auditing & System Effectiveness Evaluation	Yes	No	Yes	Yes
Hardware Redundancy	Yes	No	No	No
Data Backup	Yes	Yes	Yes	Yes
Business Continuity	Yes	No	No	No

Legend: Yes = Available; No = Not Available

Table IV- Enterprise-I data & Calculations

Months	Downtime (hrs)	Up time (hrs)	Availability%
January 04	82	636	88.611
February 04	10	710	98.611
March 04	10	710	98.611
April 04	14	706	98.056
May 04	10	710	98.611
June 04	10	710	98.611
July 04	15	705	97.917
August 04	10	710	98.611
September 04	10	710	98.611
October 04	10	710	98.611
November 04	10	710	98.611
December 04	10	710	98.611
Average Availability	**201**	**8439**	**97.674**

Availability % = (Uptime / (Downtime + Uptime)) *100

Table V- Enterprise-II data & Calculations

Months	Downtime (hrs)	Up time (hrs)	Availability%
January 04	1	719	99.861
February 04	12	707	98.331
March 04	1	718	99.861
April 04	30	689	95.828
May 04	1	718	99.861
June 04	1	718	99.861
July 04	49	670	93.185
August 04	1	718	99.861
September 04	9	710	98.748
October 04	1	718	99.861
November 04	37	692	94.854
December 04	1	718	99.861
Average Availability	**144**	**8485**	**98.331**

Availability % = (Uptime / (Downtime + Uptime)) *100

Table VI- Enterprise-III data & Calculations

Months	Downtime (hrs)	Up time (hrs)	Availability%
January 04	24	720	96.774
February 04	0	720	100.000
March 04	4.75	715.25	99.340
April 04	24	696	96.667
May 04	42	678	94.167
June 04	0	720	100.000
July 04	24	696	96.667
August 04	0	720	100.000
September 04	4	716	99.444
October 04	24	696	96.667
November 04	0	720	100.000
December 04	31	689	95.694
Average Availability	**177.75**	**8486.25**	**97.952**

Availability % = (Uptime / (Downtime + Uptime)) *100

Key determinants proposed in the model and those adopted by the enterprises are an ample proof of its affective deployment. The annual downtime of the three enterprises is depicted in tables IV, V, VI [5]. It is evident from the percentage of availability that keeping the downtime low will increase the availability. As we focus on the availability it will help reducing financial losses, thereby, provides greater productivity.

X. CONCLUSION

Information availability was not given its due share in the enterprise world due to reasons unknown and not understood. Confidentiality and integrity has been generally talked about, however, it was analyzed that with the passage of time and with ever rising competition between rivals to get more and more business, information availability is one of the major aspects which cannot be ignored and need serious looking in to. The key determinants identified in the proposed model and validated by studying in the three enterprises selected with varying business interests. The revenue of losses incurred by the said organizations highlight the significance of the information availability. It is envisaged that by implementing the proposed model, organization may achieve five nines. Information availability must be addressed effectively in the security policy to accrue full benefits of the businesses.

REFERENCES

[1] Jim Simmons, Integrating Continuity and Recovery with Information Security: *Your Best Defense for Computer Infrastructures, SunGard Availability Services* White Paper Series, (2003).

[2] "Understanding the Fundamentals of Managed Availability", *Business continuity solution series, A vision solutions* white paper (March 2004)

[3] Tryfonas, T. Grilzalis, D. & Kokalakis, S. " A quantitative approach to information availability", *proc. information security for global information infrastructure, IFIP TC11, Sixteenth annual working conference on information security,* USA, 37-47 (2000)

[4] Lampson, B.W. "Computer security in the real world", *Proc. the 16th Annual Computer Security Applications Conference*, USA (2000). Available: http://acsac.org/invited-eassy/eassys/2000-lampson.pdf

[5] M. Wasim Qureshi, "Information Availability Modeling on Enterprise Networks"

[6] Generally Accepted System Security Principles (GASSP), *International Information Security Foundation,* Generally Accepted System Security Principles Committee (June, 1997).

[7] Brinkley, D.L. & Schell, R.R, "Concepts and Terminology for Computer Society", In M.D.Abrams, S. Jajodia & H.J. Podell (Eds.), Information Security: An integrated collection of eassys, 11-39. Los Alamitos, *CA:IEEE Computer Society Press*, (1995).

[8] Mclean, J., Meadows, C., "The Future of Information Security", Center for High Assurance Computer Systems, Naval Research Laboratory, Washington, DC, USA.

[9] Information Security Guidelines for NSW Government, Part-2, Examples of Threats and Vulnerabilities, Office of Information and Communication Technology, Australia, (June, 2003).

[10] Candea, G., "Principles of dependable computer systems – the basics", Stanford University, USA, (September, 2003)

[11] ISSO Glossary of INFOSEC and INFOSEC Related Terms, Vol. I (1996).

[12] "Cisco Cable IP Solutions for High-Availability Networks", Cisco System, Inc. (2003).

[13] Enrique Vargas, "High Availability Fundamentals – Enterprise Engineering", (November, 2000).

[14] Tellis, W., "Introduction to case study", The qualitative report, 3(2), (July, 1997).