THE IMPORTANCE OF DATA PROTECTION PROCESS IN THE SMALL AND MEDIUM ENTERPRISES

Omar Hassan Mohamed Saeed

The Arab Academy for Banking and Financial Sciences (AABFS), Faculty of Information Technology and Systems, Jordan

ABSTRACT

This title paper has a relation in some ways to the topic of (Managing Information Resources).This paper describes the new factors that have increased data protection risks; then demonstrate the small and midsize business's Data Protection hurt Points. It introduces some situations that if they happened, it will affect the business data; delay decision making process and by the result, it maybe interrupts the business for a period of time. Finally it introduce some recommended scientific and implemented advices according to IS and IT sciences for treating this problem and minimizing its effects in the small and midsize businesses.

Keywords: *Information system management, Information system strategy, Decision support system.*

1. INTRODUCTION

Whether you're a big financial services company or a ten-person regional service firm, you are possibly progressively more reliant on your data for your everyday processes; but there are many most important threats influencing you to protect your business's critical information; these threats include for examples: (the flood of major virus attacks, electricity power shortages and normal disasters, joint with the fewer published problems like equipment breakdowns, network disruptions or simple human error).

There are some new reasons that have enlarged data protection threats which include:-

1. The growing of business information produced daily indicates even progressively data has to be backed up.

2. Consumers imagine services to come back quickly after a business interruption; despite of the situation.

3. The growing need to contact data approximately around the clock has significantly minimized the time allowed to backup data.

Today's data protection challenge creates significant threats to firms of all sizes, but they create the most threat to small and medium enterprises.

2. DATA PROTECTION HURT POINTS

Let us have a look to Small and Medium Enterprises Data Protection hurt Points:-

2.1. Limited IT resources for backup and recovery:

Many small and medium enterprises have little or no devoted IT personnel to react rapidly to business disruptions.

2.2. All critical data on one server:

If that server falls down, most units have to get that server running and fully repaired, or face expensive results.

2.3. Regulatory pressures:

Small and medium enterprises like large corporations are subject to the same data accessibility and data security necessities; but without the sufficient resources to encounter these needs.

2.4. Cash flow interruptions:

Small and medium enterprises can not afford business interruptions that can not be rapidly recovered because of the lack of cash flow.

3. SOME REGULAR SITUATIONS THAT UNDERLINE THE THREATS TO A THRIVING MIDSIZE BUSINESS

(Tuesday 4PM): If the firm server crashes; and there is no another standby server; so; users can not access e-mail, the customer database, or their project directories.

3.1. Best Case Situation

(Tuesday Evening): The reseller arrives with parts needed to fix the server and restores the new server from the Monday night tape backup.

(Wednesday Morning): Users can restart work; but all of Tuesday's data has been lost and a few hours lost of productivity.

3.2. More Likely Situation

(Wednesday Afternoon): The reseller did not have all of the parts in stock; so; he call for replacement parts, but it did not arrive until Wednesday afternoon, the reseller fixes the server and tries to restore from the Monday night tape backup.

(Thursday Morning): Users can restart work, but the most recent data they can access is from Monday night and a day lost of productivity.

3.3. Worst Case Situation

(Wednesday Afternoon**)**: The reseller did not have all of the parts in stock; so; he call for replacement parts, but it did not arrive until Wednesday afternoon, the reseller fixes the server and tries to restore from the Monday night tape backup; but the Monday night tape is bad, so he have to restore from Sunday night's tape.

(Thursday Morning**):** Users can restart work, but they can not access data from later than last weekend and a day lost of productivity, but the firm lost everything of its data since last weekend.

4. SO; WHAT CAN A SMALL OR MEDIUM ENTERPRISES DO TO REDUCE THIS HUGE THREAT TO THEIR BUSINESS?

Of course there are many solutions refer to the specialty of the firm, but I think that every small and medium enterprise must take these following advices on their thinking while protecting their critical information.

4.1. First advice: (Getting the right People, Policies and Priorities)

The medium enterprise must have the right people, policies and procedures in place, by means of the" data protection owner", which should be responsible for documenting the processes, investigating the options, and directing the testing and training.

The "data protection owner" should form a group including, a manager from each unit to determine what is the most critical information to the business, (in a small business, this may be just the owner, or the executive staff).

The "data protection owner" should identify any relevant regulations that affect the company's data protection priorities, and the group should define the critical applications.

Because of the limited resources in most small and medium enterprises, this group should initially narrow their focus to one or two core applications where an inability to access key information can quickly start to cost their business money (e.g. the business e-commerce site? the customer database? the e-mail system?) to make the most important data protection goals more attainable.

4.2. Second advice: (Thinking about the place of business Data

It is extremely important that the business can put its data out of harm's locations. The ideal offsite location is distant geographically, so it remains unaffected by large-scale disasters, such as earthquakes and hurricanes.

The firm must consider the most likely threats to its place such as:-

-The electricity power shortages; then how far away would it need to store the data to be on a different power grid?

-Earthquakes or hurricanes; then, it probably need to keep the backup data at least an area code away.

-Server failures; then what could be done for more rapid recovery of the production machine?

The firm must think creatively about how it can cost effectively backup the data remotely.

4.3. Third advice: (Estimating the downtime)

The firm may need to estimate the downtime costs for its employees, suppliers and customers who they are not being able to access the critical information, and then the senior management must understand the downtime cost estimation to agree on the data protection budget.

The following method provides a simple way for a business to conventionally estimate the average cost per hour of downtime for each critical application:

(Simple Downtime Estimate Formula):-

{Productivity Impact + Revenue Impact = Downtime Estimate}

While as:-

Productivity Impact: Average worker rate or salary **X** estimated number of business hours the users would be impacted.

Revenue Impact: Average monthly gross revenue for the critical application **X** number of business hours the application is impacted.

Next, the business should consider defining the recovery objectives for its applications. The best way to quantify business objectives is with a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each application.

The RTO for an application is simply the goal for how quickly the business need to have that application's information back available after downtime has occurred; for example, for the e-mail system is it 4 hours, 8 hours or next business day?

The RPO for an application is the goal for how much data the business can afford to lose since the last backup; is it 2 minutes worth, 20 minutes or 2 hours?

The business then needs to roughly estimate the costs to achieve its RTO and RPO for each application.

The last and most important part, the business need to get the senior management understands and agreement with the downtime cost estimates and required RTO and RPO goals. Once everyone has agreed on the "Costs of

Downtime" and the company's RTO and RPO goals, and then it's easier for everyone to agree on the data protection budget. For example, if can get the business owner or executive team's agreement that the company's downtime costs are approximately $100,000 per year, they are more likely to agree that $50,000 is an appropriate data protection budget.

4.4. Fourth advice: (Thinking about IT solution)

Because many small and medium enterprises ever more dependent on their data, the business is likely to discover that traditional tape backup won't be good enough to achieve its RTO and RPO goals for its most critical applications.

For small and medium enterprises whose critical application runs at multiple remote locations (such as retail stores or bank branches) the quality and consistency of on-site tape backup is also important.

But few companies of any size have the technical experts in branch locations that can check that the tapes are properly backing up, maintain and clean tapes, and execute a recovery.

Small and medium enterprises maybe use a backup system which is inexpensive and reasonably reliable, but it offer poor RPO and RTO for critical applications, and it is usually ineffective for remote locations.

Hardware mirroring technology (which use remote copy technology to provide synchronous mirroring between two sites) offer excellent RPO and RTO ;but it is prohibitively expensive for a small or medium enterprise to buy and manage, plus, it is less than ideal for backing up remote locations, which often have low-bandwidth connections.

The firm must think creatively about technology solution, the business can now select the appropriate technology solution and implementing it to protect its critical information because of the wide availability of numerous IT innovations.

5. CONCLUSIONS AND RECOMMENDATIONS

Like major corporations, small and medium enterprises are progressively more dependent on the essential data stored on their servers, but because of their limited IT resources and their greater exposure to disruptions, small and medium enterprises are even more at risk. In the past, small and medium enterprises often had to live with this greater level of threat, but now a day this is no longer true because of the wide availability of numerous IT innovations combined with the progress in the IS science.

Small and medium enterprises can now implementing some simple scientific advices like those suggested in this paper, and can selecting new available IT solutions which can significantly reduce firm's downtime threats and protect business critical information necessary to the decision making process.

While this research paper was discussing one area that refer to small and medium enterprises, I hope that academic researchers and industry developers will find it useful and will be able to base more detailed work on this subject.

7. REFERENCES

[[1] Anderson, D. (2000), Managing Information Systems, Prentice-Hall, Englewood Cliff, NJ

[2] Barbara C. McNurlin. & Ralph H. Sprague, Jr. Information System Management in Practice (6th Ed). Pearson Prentice Hall.

[3] Brynjolfsson, E., Malone, T. Gurbaxani, V. and Kambil, A., "Does information technology lead to smaller firms?" Technical Report 106, Center for coordination Science, MIT, 1989.

[4] Edwards, B. (1994), "Developing a successful disaster recovery plan", Information Management and Computer Security, Vol. 2 No.3.

[5] Fitzgerald, K.J. (1994), "The importance of a network disaster recovery plan", Information Management and Computer Security, Vol. 2 No.1.

[6] Heng, G.M. (1996), "Developing a suitable business continuity planning methodology", Information Management and Computer Security, Vol. 4 No.2.

[7] Home Office (1997), Dealing with Disaster, 3rd ed., Brodie Publishing, Wellington.

[8] J. Budzik and K.J. Hammond. User interactions with everyday applications as context for just-in-time information. Access. In Proc. of Intelligent User Interfaces 2000. ACM Press, 2000.

[9] Keen, Peter, Every Manager's Guide to Information Technology, Harvard Business School Press, Boston, MA, 1991.

[10] Moore, P. (1995), "Critical elements of a disaster recovery and business/service continuity plan", Facilities, Vol. 13 No.9.

[11] Simon, J.C. (2001), Introduction to Information Systems, John Wiley & Sons, New York, NY.[12] Toigo, J. (1996), Disaster Recovery Planning for Computers and Communication Resources, John Wiley, & Sons, New York, NY.