https://doi.org/10.48009/1_iis_2018_20-28
Issues in Information Systems
Volume 19, Issue 1, pp. 20-28, 2018

DATA BACKUP: DO BUSINESSES WANT TO MEASURE RECOVERY POTENTIAL?

Gwen White, Xavier University whiteg@xavier.edu
David White, Xavier University whited4@xavier.edu

ABSTRACT

It is increasingly important to understand the significance of the ability of a company to restore data after a disaster. Reports reveal many organizations cannot fully restore data after a disaster, be them by nature or human oversight. There are hardware failures, human error, or hacking that require an action plan that can deter or vanquish the failure of data backup success. Many businesses do not backup their data on a proper schedule nor do they use the proper procedures for storage after backing up. This paper introduces the concept of a data backup indicator that assists management and IT specialists to understand the reliability of the restoration of a data backup for businesses that backup data in-house. The data backup indicator is based on Six Sigma principles and is calculated based on files in a data backup. The data was analyzed using binary logistic regression. The results indicated there was a positive linear relationship related to the size of the company and the desire for the data backup indicator.

Keywords: Disaster Recovery, Data Backup, Failed Backup Recovery, Data Backup Indicator

INTRODUCTION

Businesses are vulnerable to disasters whether they are caused by humans or a natural phenomenon (Nelson, 2011). Disasters are not scripted or scheduled and usually catch companies off guard. Human disasters including but not limited to denial of service, viruses, ransomware, lack of job knowledge. Natural disasters including but not limited to fires, floods, wind, tornadoes and earthquakes (Symantec, 2011). The Federal Emergency Management Agency (2017) documented over 3,300 disasters between 1976 to 2017. At the time of restoration many companies could not return to full operations due to an insufficient or unreliable data backup.

The objective of this study is to investigate if there is a relationship between the desire for a data backup performance indicator measurement tool and the size of the organization for businesses that backup data either online or in house. There is literature that discusses why organizations create disaster recovery plans (DRPs) and business continuity plans (BCPs) and backup up data as a part of a disaster recovery strategy. Organizations test the DRPs, BCPs and data backups but when a disaster occurs, many still cannot recover (Symantec 2012). The possibility of quantification of the data backup could potentially assist in the recovery process.

Overall, data backup managers do not quantify data backup. The lack of quantification affects the line of communication between the data backup manager and company management. If a data backup manager states the data backup was successful, mangers tend to believe that the data backup was perfect (Gartner, 2013). A backup performance indicator benchmarks the data backup to provide a platform for evaluating the condition of its backup. The data backup performance indicator is based on Six Sigma principles which explained the accuracy of the data backup for business. Creating a backup performance indicator (quantification) can help management understand the data backup process and the potential for recovery after a disaster.

Disaster Recovery, Data Backup, Six Sigma and Data Backup Indicator

Research had not been conducted to determine the need for a data backup performance indicator that explained the accuracy of the data backup for business. The articles reviewed contained information on ways to back up data, prepare a disaster backup plan, improve the data backup process, and the number of organizations that currently back up their data. The existing literature did not contain information on effective communication between data backup personnel or the need for a data backup indicator.

Disaster Recovery Theory

Disaster recovery principles were created in the 1970s when the organizational use of computing technology was first becoming pervasive with massive amounts of data generated. Any interruption to computing services resulted in loss of data with financial repercussions. The ability to return to operations quickly without data loss was important to businesses (Esnard & Sapat, 2014). For this reason, the disaster recovery industry grew in the 1980s and 1990s, along with government regulations that mandated Disaster Recovery Plans (DRPs) including a long-term business continuity plan (BCP). Use of the Internet increased in the 2000s, which in turn increased the importance of DRPs to ensuring the availability of computing systems.

Classical disaster recovery, which established roots in emergency and disaster management, typically included four components: mitigation, preparedness, response, and recovery. In this model, there was no performance measurement designed to reduce or eliminate the risk from disasters. Preparedness meant the overall ability or readiness to respond to emergencies or crises, response referred to the action taken to prevent further damage in an emergency, and recovery referred to the ability to return to normal operations including any reconstruction or rebuilding (Esnard & Sapat, 2014). When organizations created a DRP, they used all four components to ensure that business returned to operations within a reasonable amount of time. One of the potential issues, however, was whether the data backup portion of such an operation was viable.

A DRP encompasses all the tools necessary to return to functionality, including personnel coordination, alternate locations for operations, plan testing, and assignment of responsibility. DRP methodology for recovering from a disaster included a backup plan, a BCP, and a contingency plan for downtime (Nollau, 2009). Nollau (2009) and Engemann and Henderson (2012) agreed that a DRP focuses on the restoration of technology to functionality before a disaster. A backup plan focuses on the maintenance of company data and records stored in various on- or off-site media. A BCP creates a map to restore business processes to their pre-disaster levels. A contingency plan helps an organization move operations in case of a disaster, allowing the business to operate temporarily in another location until the organization returns to regular operations (Engemann & Henderson, 2012).

DRPs involve a process that incorporates teamwork, a designated leader, and a sponsor. The sponsor initiates the DRP, which was designed by the business continuity manager. The sponsor of the DRP is an executive responsible for the implementation of the planning process. The business continuity manager (designated leader), meanwhile, is responsible for ensuring the completion and frequent updates of the project (Hiatt, 2000). Finally, a team is created to incorporate the various departments that would be affected by a disaster.

For example, the team includes senior managers who are knowledgeable about the damaged facility, voice communication, and information technology personnel. These senior managers lead the restoration process. Risk analysis includes the identification of threats to assets and business functions. In such an analysis, all assets are identified along with potential damage to the business if a particular asset fails due to a disaster (Larrue, Kummer, Müller, & Bluhmki, 2011). The DRP is designed to include various tasks and activities that help an organization return to regular operations after risk assessment. It is the responsibility of the business continuity manager to consistently test the DRP and to keep it updated (Larrue et al., 2011). Finally, a plan should be documented and implemented when a disaster occurs.

Backup Theory

A backup is a snapshot of data at a particular time, and the size of a backup changes depending on the number of files it incorporates. There is a variety of backup methods including full, differential, and incremental. A full backup copies all files on a drive. A differential backup copies only files that have changed since the last full backup. An incremental backup copies files that have changed since the last incremental or full backup (Nelson, 2011).

An archive refers to the long-term storage of backup data. It is an original file moved to another location. Archived data does not change over the long term and is restored if necessary at a later date (Nelson, 2011). At the end of a backup cycle, the unused data are copied to another medium and stored for long-term retention purposes. In the long term, the data are stored offline or in house. Archives reduce the long-term need for backup data. Popular locations for archived data backup include CD-ROMs/DVDs, storage area networks (SANs), hard drives, and cloud backups. Cloud backups are the most economical and convenient of all the methods due to the accessibility of the cloud from remote locations (Omar et al., 2011).

Traditionally, data were copied from one medium to another. The first data backups occurred in the 1950s and involved duplicating and storing punch cards for later restoration (Nelson, 2011). Magnetic tapes replaced punch cards in the 1960s. Magnetic tapes stored more data (10,000 punch cards per tape) and were not as volatile. Magnetic tapes were widely used until the 1980s and are still in use today in some applications. In the 1960s, the industry introduced floppy drives as an option for backing up files on a smaller scale (EC-Council, 2011). Floppy drives for disk storage were used primarily for computer-to-computer file exchanges. Small businesses and home users were the primary benefactors of floppy disk storage and backup. However, backing up to floppy disks required many disks, which were difficult to store and could easily fall out of order.

By 1979, compact discs (CDs) replaced floppy drives as the next storage medium, and by 1990 CDs stored 740 MB of data (Nelson, 2011). Later, DVDs were introduced, which allowed up to 4 GB of data on a single disk. Hard drives were the next media used to back up data. In the 1960s and 1970s, hard drives were not large enough and were too expensive for data backup. By the 1990s, however, hard drives increased in capacity, and their prices dropped. This allowed for their use as viable locations for data backup and redundant arrays of inexpensive disks (RAIDs), which were used to store data due to their low cost and high storage capabilities.

Network and online data storage systems were the next methods for storing backup data. Local area networks (LANs) and wide area networks (WANs) allowed backup to remote locations. By 1992, network-attached storage (NAS) had become popular, along with storage area networks (SANs) using high-speed immediate backup for larger enterprises (Nelson, 2011; Purushothaman & Abburu, 2012). SANs were very effective because they allowed connection to remote targets such as hard drives and tapes on a network.

The typical backup operator backs up data without incident. However, when everything is working, management tends to perceive the backup operator as a drain on resources with no income-generating purpose. Backups then remain dormant until a disaster occurs, at which point their job becomes critical (Symantec, 2012). The job of the backup operator is "invisible," especially when everything is working properly (Nelson, 2011). The ability to use a quality management measurement program that shows how important backups are to an organization is vital to that organization's long-term survival. Technology is the most automated and easy-to-manage part of a backup system (deGuise, 2008). Conversely, human interaction is the most detrimental to a backup system, even when people minimize the amount of time spent interacting with the system (deGuise, 2008).

Symantec's Disaster Preparedness Survey (2011) assessed a variety of organizations and reported that data were either not backed properly up or not backed up at all and found that only half of organizations backed up 60% of their data. Many either backed up all their data or picked the data they wished to save. Thirty-one percent did not back up e-mail, 21% did not back up their application data, and 17% did not back up their customer data (Symantec Corporation, 2011). Fewer than 50% of surveyed companies backed up their data once per week and only 23% backed up their data daily.

Other problems in businesses included improper storage of media or theft of media, which rendered them unusable for restoration (Symantec, 2012). Integrity issues involved skipped or corrupted files, a missing backup schedule, and tape destruction. Further, organizations did not always test their data backups to ensure that they were fully functional and that they flowed correctly. This lack of testing led to future problems if some portions of the plan were not ready to be implemented to bring the organization back to productivity.

Organizations must develop a backup plan and not just use a series of backup software products (deGuise, 2008). Data that were backed up must be consistent, not skipped over or changed. An organization must address policies, procedures, people, and attitudes to ensure that the backup plan was high quality, redundant, consistent, and functional (deGuise, 2008).

Six Sigma

Six Sigma, created by Pyzdek (2003), was based on studies of Japanese organizations such as Motorola showing that their quality processes were significantly better than those of U.S. organizations. Six Sigma emphasized continuous improvement, controls, and top management commitment to improving quality and reducing costs within an organization. Organizations strived to achieve Six Sigma quality and must not exceed 3.4 defects per million opportunities (Pyzdek, 2003). A single Sigma was 690,000 defects per million opportunities or one standard deviation

from the mean. The greater the number of standard deviations between the mean and the nearest specification, the lower the number of sigmas (see Figure 1). Anything less than six standard deviations did not meet the Six Sigma standard of quality (Pyzdek & Keller, 2014).

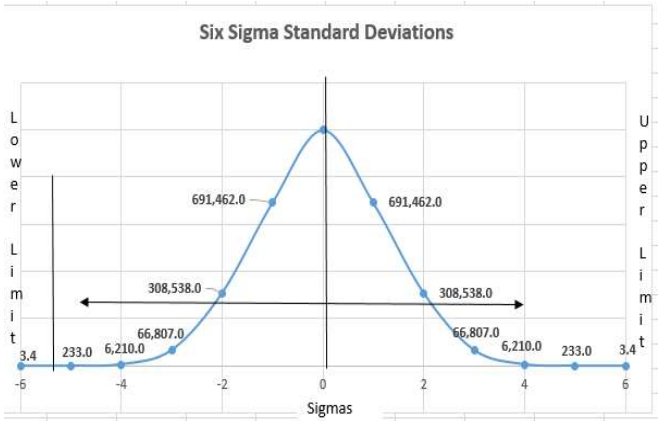


Figure 1. Six Sigma Standard Deviations (Pyzdek, 2003).

There were many Sigma levels for a project: 4α was 6,210 defects per million opportunities; 5α, 233 defects per million; and 6α, 3.4 defects per million opportunities (Pyzdek, 2003). The goal was to achieve a Six Sigma level for many of the individual processes in the organization. There were two methodologies used in Six Sigma to create change: (a) define, measure, analyze, improve, and control (DMAIC); and (b) design, measure, analyze, design, and verify (DMADV) (Pyzdek & Keller, 2014). In a disaster recovery scenario, either of these methodologies were used as a foundation to develop a way to measure the quality of a plan. These methodologies made the plan more efficient by decreasing the number of its defects. Why not take the principles of Six Sigma and apply them to data backup to ensure recovery or at least an understanding of the potential to recover after a disaster?

Organizations which used Six Sigma found the information in this study valuable to their bottom line. Therefore, it seemed that using a data backup indicator measurement tool could become a standard for all industries that use data backups. For this reason, it was important for management to understand data backup and not to rely solely on the IT department to provide an accurate measurement. Existing data backup plans were not quantified into an easily measurable system whereby all non-IT personnel could understand the current status of the plan. A data backup indicator based on Six Sigma mathematics would be easily quantifiable.

Six Sigma is used in a variety of environments and for a variety of applications, including standardizing data backup systems. A Six Sigma backup system features a multitude of components including technologies, processes, people, documentation, service-level agreements, and testing (deGuise, 2008). The need for such a backup process is important because the amount of data that organizations store increases each year. Companies began to specialize in such data backup systems as Exabyte in the 1970s, Remote Backup Systems in 1987, IBM Tivoli in 1993, and Veritas/Symantec in the 1990s. CommVault, EVault, Acronis, Arkeia, Carbonite, Dell Backup, and more have been created to meet growing demand.

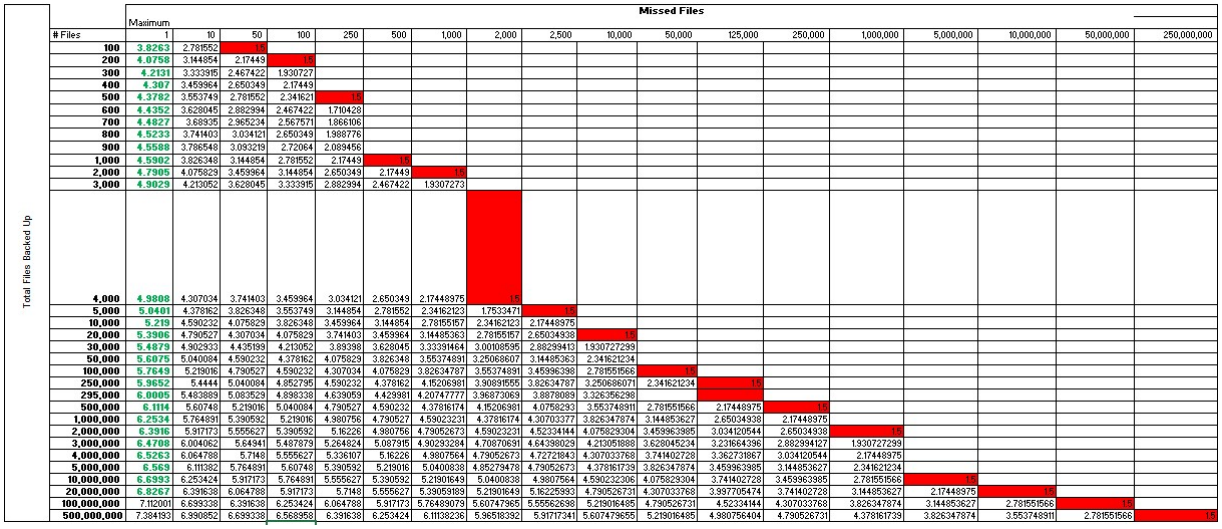
Data Backup Indicator

The creation of a backup performance indicator provided labeling information to help determine if the data backup was useful in a crisis. The information gathered helped businesses to understand the importance of confidence in the quality of the data backup as well as the need for a backup performance indicator. The study was designed to determine if there was a positive linear relationship between the size of a business and their desire for a data backup indicator. The data backup indicator would be based on the number of files backed up and the success rate of those backups. The formula used to calculate the DBI is:

Data Backup Indicator (DBI) =NORMSINV(1-(Number of Files Missed/Number of Files Backed))+1.5 Sigma Shift

Each backup session has a DBI number that indicates the highest level of backed up files. For example, if there were a total of 1,000,000 files, the highest DBI will be 6.2534 which indicates only one file was missed in the backup. The

lowest possible number is 1.5 (Sigma Shift) indicating that Six Sigma is 0. The backup administrator should strive for the highest DBI number (Figure 2). The more files missed the lower the DBI number which indicates the data backup process needs improvement. The DBI allows management to understand the backup process and its current state.



Total Files Backed Up	Maximum	Missed Files: 1	10	50	100	250	500	1,000	2,000	2,500	10,000	50,000	125,000	250,000	1,000,000	5,000,000	10,000,000	50,000,000	250,000,000
# Files																			
100	3.8263	2.781552	1.5																
200	4.0758	3.144854	2.17449	1.5															
300	4.2131	3.333915	2.467422	1.930727															
400	4.307	3.459964	2.650349	2.17449															
500	4.3782	3.553749	2.781552	2.341621	1.5														
600	4.4352	3.628045	2.882994	2.467422	1.710428														
700	4.4827	3.68935	2.965234	2.567571	1.866106														
800	4.5233	3.741403	3.034121	2.650349	1.988776														
900	4.5588	3.786548	3.093219	2.72064	2.089456														
1,000	4.5902	3.826348	3.144854	2.781552	2.17449	1.5													
2,000	4.7305	4.075829	3.459964	3.144854	2.650349	2.17449	1.5												
3,000	4.9029	4.213052	3.628045	3.333915	2.882994	2.467422	1.9307273												
4,000	4.9888	4.307034	3.741403	3.459964	3.034121	2.650349	2.17448975	1.5											
5,000	5.0401	4.378162	3.826348	3.553749	3.144854	2.781552	2.34162123	1.7533471	1.5										
10,000	5.219	4.590232	4.075829	3.826348	3.459964	3.144854	2.78155157	2.34162123	2.17448975										
20,000	5.3906	4.790527	4.307034	4.075829	3.741403	3.459964	3.14485363	2.78155157	2.65034938	1.5									
30,000	5.4879	4.902933	4.435199	4.213052	3.89398	3.628045	3.33391464	3.00108595	2.88299413	1.930727299									
50,000	5.6075	5.040084	4.590232	4.378162	4.075829	3.826348	3.55374891	3.25068607	3.14485363	2.341621234									
100,000	5.7649	5.219016	4.790527	4.590232	4.307034	4.075829	3.82634787	3.55374891	3.45996398	2.781551566	1.5								
250,000	5.9652	5.4444	5.040084	4.852795	4.590232	4.378162	4.15206981	3.90891555	3.82634787	3.250686071	2.341621234	1.5							
295,000	6.0005	5.483889	5.083529	4.896338	4.639059	4.429981	4.20747777	3.96873069	3.8878089	3.326356238		1.5							
500,000	6.1114	5.60748	5.219016	5.040084	4.790527	4.590232	4.37816174	4.15206981	4.0758293	3.953749911	2.781551566	2.17448975	1.5						
1,000,000	6.2534	5.764891	5.390592	5.219016	4.980756	4.790527	4.59023231	4.37816174	4.30703377	3.826347874	3.144853627	2.65034938	2.17448975						
2,000,000	6.3916	5.917173	5.555627	5.390592	5.16226	4.980756	4.79052673	4.59023231	4.52334144	4.075829304	3.459963985	3.034120544	2.65034938	1.5					
3,000,000	6.4708	6.004062	5.64941	5.487879	5.264824	5.087915	4.90293284	4.70870691	4.64398029	4.213051888	3.628045234	3.231664396	2.882994127	1.930727299					
4,000,000	6.5263	6.064788	5.7148	5.555627	5.336107	5.16226	4.9807564	4.79052673	4.72721843	4.307033768	3.741402728	3.362731867	3.034120544	2.17448975					
5,000,000	6.569	6.111382	5.764891	5.60748	5.390592	5.219016	5.0400838	4.85279478	4.79052673	4.378161739	3.826347874	3.459963985	3.144853627	2.341621234					
10,000,000	6.6393	6.253424	5.917173	5.764891	5.555627	5.390592	5.21901649	5.0400838	4.9807564	4.590232306	4.075829304	3.741402728	3.459963985	2.781551566	1.5				
20,000,000	6.8267	6.391638	6.064788	5.917173	5.7148	5.555627	5.39059189	5.21901649	5.16225993	4.790526731	4.307033768	3.997705474	3.741402728	3.144853627	2.17448975	1.5			
100,000,000	7.112001	6.699338	6.391638	6.253424	6.064788	5.917173	5.76489079	5.60747965	5.55562698	5.219016485	4.790526731	4.52334144	4.307033768	3.826347874	3.144853627	2.781551566	1.5		
500,000,000	7.384193	6.990852	6.699338	6.568958	6.391638	6.253424	6.11138236	5.96518392	5.91717341	5.607479655	5.219016485	4.980756404	4.790526731	4.378161739	3.826347874	3.553748911	2.781551566	1.5	

Figure 2. DBI Indicator Measurement Table

Management and backup personnel do not apply quantification to data backups which can lead to failed data restoration attempts. This lack of data backup quantification led to inadequate data restoration, which led to loss of revenue, productivity and/or total business shutdown. Businesses that experienced such data loss often closed within two years of the disaster (Snedaker & Rima, 2014).

RESEARCH METHODOLOGY

This is a quantitative study using a logistic regression (Lund Research, 2017). The target population for this study were businesses that used computers with data backup operations within the past 30 days and/or have attended a data backup/disaster recovery conference in 2016. The population selected was N=250 and the sample size returned was n=53.

A modified online validated instrument from Information Week was used to assess the need for a data backup indicator. One additional question was added to assess the need for a data backup indicator. The independent variables for this study included the size of the company. The dependent variable for the study was the need for a data backup performance indicator. The companies were classified into the following groups based on size (Table 1).

Table 1. Business Groupings

Group #	Business Size
1	1-250
2	251-500
3	501-750
4	751-1000
5	> 1000

Hypothesis:
H_0: There is no positive linear relationship between the size of a business and their desire for a data backup indicator (as the business size grows the desire for a data backup indicator does not grow) $\beta_i \neq 0$

H_A: There is a positive linear relationship between the size of a business and their desire for a data backup indicator (as the business size grows the desire for a data backup indicator grows) $\beta_i > 0$

The research consisted of collecting quantitative survey data from data backup operators. The binary logistic regression equation for this study is logit(need for dbi) = $\alpha + \beta_1$NUMBEREMPLOYEES emphasizing that the size of the business will be the primary predictor.

RESULTS

A binomial logistic regression was performed to ascertain the effects of business size on the desire for a data backup indicator. The log of the odds of a company choosing the use the data backup indicator was positively related to size of the company and statistically significant. The variable numberemployees was significant p<.05 The Omnibus Test of Model Coefficients logistic regression model was statistically significant $X^2(2) = 21.353$ p<.05 (Table 2).

Table 2. Omnibus Test of Coefficients

Chi-Square	21.35312712
df	1
p-value	3.81997E-06
alpha	0.05
sig	yes

The Hosmer-Lemeshow Test indicated that the model was (p >.05) indicating the model $X^2(2) = 1.565$ p > .05 was insignificant indicating the model was a good fit (Table 3).

Table 3. Hosmer-Lemenshow

Hosmer-Lemenshow	1.565300474
Df	2
p-value	0.457192735
Alpha	0.05
Sig	no

The model explained 44.65% (Nagelkerke R^2) of the variance in the desire and correctly classified 75.47% of cases (Table 4). The R^2 is slightly below 50% indicating that the model is moderately predictive, but in this case, it will be used until further research is conducted.

Table 4. R^2 Output

R-Sq (L)	0.296827355
R-Sq (CS)	0.331613841
R-Sq (N)	0.446527758

Sensitivity was 70.96%, specificity was 81.81% positive predictive value was 70.97% and negative predictive value 81.82% (Table 7). The size of the business had 2.6023 odds of saying yes (0 = no 1 = yes) to the need for the data backup indicator. Therefore, the larger the business the more likely they would say “yes” to the data Logit(y)=-1.7125+.9564(numberemployees) (Table 5).

Table 5. Logistic Regression Output

	coeff b	*s.e.*	*Wald*	*p-value*	*exp(b)*	*lower*	*upper*
Intercept	-1.7125	0.5783	8.7689	0.0031	0.1804		
Numberemployees	0.9564	0.2772	11.9002	0.0006	2.6023	1.5114	4.4808

Based on the output of the data, all classes were correctly classified regarding their desire for the data backup indicator. The data groupings were displayed with their success and failures of the need for a data backup indicator. Observations probabilities were computed using $p=1/1+e^{-b0-b1x1}$. Employees with 1 to 50 employees did not desire the data backup indicator (9 success, 18 failure) and those with over 1,000 employees wanted the data backup indicator (13 success, 1 failure), therefore proving the alternative hypothesis that there is a positive linear relationship between the need for a data back indicator and number of employees.

Table 6. Logistic Regression Grouping Output

Number of Employees	*Success*	*Failure*	*Total*	*p-Obs*	*p-Pred*	*Suc-Pred*	*Fail-Pred*	*LL*	*% Correct*	*HL Stat*
1	9	18	27	0.3333	0.3195	8.6265	18.3735	-17.1977	66.6667	0.0238
2	2	3	5	0.4000	0.5499	2.7496	2.2504	-3.5909	40.0000	0.4540
4	7	0	7	1.0000	0.8922	6.2452	0.7548	-0.7986	100.000	0.8460
5	13	1	14	0.9286	0.9556	13.3787	0.6213	-3.7051	92.8571	0.2415
Totals	31	22	53			31.00	22.00	-25.2924	75.4717	1.5653

Table 7. Classification Table

	Suc-Obs	Fail-Obs	Totals
Suc-Pred	22	4	26
Fail-Pred	9	18	27
Totals	31	22	53
Accuracy	0.709677419	0.818181818	0.754716981
**Cutoff	0.5		

LIMITATIONS

This was a small and focused sample in relation to the total business population. The quantitative method limited the ability to reveal specific details of the small businesses selected. The population and sample were selected from those that attended the conference and with a change of location, it might be possible to obtain different results. One of the limitations of quantitative studies that include self-reported information may be incomplete or inaccurate data (Jaggia & Kelly, 2016). It was likely that participants under reported their actual data backup instances. In addition, the inflexibility of the questions did not allow for any changes once the survey started; therefore, a qualitative or mixed-methods study might be appropriate to address this problem.

CONCLUSION

Disasters cannot be avoided. Organizations should prepare for a successful data backup restoration. This article examined the desire to use a data backup indicator in relation to the size of a business. The results of the study indicated that there is a positive linear relationship between the size of the business and their desire to use the data

backup indicator. The larger the organization the more the desire for the DBI. However, organizations are overwhelmed with day to day business. Whether it is intentional or unintentional, data backup and disaster recovery are a priority. Recovery efforts can be hampered, even if companies thought they were prepared. The use of a data backup indicator might help organizations understand the current state of the data backup in relation to recovering from a disaster. It is hoped that this data backup indicator will become a tool that is used regardless of business size to assist management and IT with restoration understanding in case of a disaster.

REFERENCES

Alliance Storage Technologies. (2007). *Case study: Hospital's data survives hurricane Katrina.* Retrieved from Alliance Storage Technologies: http://www.plasmon.com/downloads/pdf/katrinacasestudy.pdf

Arizona Emergency Management. (2011). *Arizona emergency management.* Retrieved from Arizona emergency management: http://www.dem.azdema.gov/operations/mitigation/mitigation.html

deGuise, P. (2008). *Enterprise systems backup and recovery: A corporate insurance policy.* Sydney, Australia: Auerbach Publications.

EC-Council. (2011). *Disaster recovery.* Clifton Park, NY: Cengage Learning.

Engemann, K. J., & Henderson, D. M. (2012). *Business continuity and risk management.* Brookfield, CT: Rosthsteiin Associates Incorporated.

Esnard, A. M., & Sapat, A. (2014). *Displaced by disaster: Recover and resilience in a globalizing world. Environmental crises, population displacement, and disaster recovery.* New York, NY: Routledge.

Federal Emergency Management Agency. (2017). *Disaster declarations by year*. Retrieved January 2018, from Federal Emergency Management Agency: https://www.fema.gov/disasters/year.

Gartner Group. (2013). *Predicts 2014: Business continuity management and IT disaster recovery management.* Stamford, CT: Gartner Group.

Gijo, E. V., Scaria, J., & Antony, J. (2011). Application of Six Sigma methodology to reduce defects of a grinding process. *Quality & Reliability Engineering International., 27*(8), 1221-1234.

Gijo, E., & Sarkar, A. (2013). Application of Six Sigma to improve the quality of the road for wind turbine installation. *The TQM Journal, 25*(3), 244-258.

Goh, T. N. (2011, March). Six Sigma in industry: Some observations after twenty-five years. *Quality & Reliability Engineering International, 27*(2), 221-227.

Goldsborough, R. (2012). Preparing for the next emergency. *Teacher Librarian, 40*(2), 68.

Hiatt, C. J. (2000). *A primer for disaster recovery planning in an IT environment.* Hershey, PA: Idea Group Publishing.

Ismail, M., & Alias, S. (2014). Binary logistic regression modeling: Measuring the probability of relapse cases among drug addicts. *AIP Conference Proceedings, 1605*, 792-797.

Jaggia, S., & Kelly, A. (2016). *Business statistics: Communicating with numbers. Second edition.* New York, NY: McGraw Hill.

Larrue, V., Kummer, R. v., Müller, A., & Bluhmki, E. (2011). Risk factors for severe hemorrhagic transformation in ischemic stroke patients treated with recombinant tissue plasminogen activator: A secondary analysis of the

European-Australasian acute stroke study (ECASS II). *Journal of the American Heart Association, 32*, 438-441. doi:10.1161/01.STR.32.2.438

Lund Research. (2017, January 20). *Laerd Statistics*. Retrieved January 20, 2017, from Laerd Statistics: https://statistics.laerd.com/premium/spss/blr/binomial-logistic-regression-in-spss.php

Marks, H. (2014). *2014 Backup Technologies Survey.* Chicago, IL: Information Week.

Nelson, S. (2011). *Pro data backup and recovery.* New York, NY: Springer.

Nollau, B. (2009). Disaster recovery and business continuity. *Journal of GXP Compliance, 13*(3), 51-58.

Osborne, J. (2014). *Best practices in logistic regression.* Thousand Oaks, CA: Sage Publications.

Omar, A., Alijani, D., & Mason, R. (2011). Information technology disaster recovery plan: Case study. *Academy of Strategic Management Journal, 10*(2), 127-141.

Purushothaman, D., & Abburu, S. (2012). An approach for data storage security in cloud computing. *International Journal of Computer Science Issues, 9*(2), 100-105. Retrieved from https://www.ijcsi.org/papers/IJCSI-9-2-1-100-105.pdf

Pyzdek, T. (2003). *The Six Sigma Handbook.* New York, NY: McGraw-Hill.

Pyzdek, T., & Keller, P. (2014). *The Six Sigma handbook: Fourth edition.* New York, NY: McGraw-Hill.

Snedaker, S., & Rima, C. (2014). *Business continuity and disaster recovery planning for IT professionals.* Walthan, MA: Elsevier.

Soric, B., & Šusak, T. (2015, January). Development of dividend payout model using logistic regression: The case. *Economy Transdisciplinarity Cognition*, 117-123.

Symantec. (2012). *Disaster preparedness survey.* Mountain View, CA: Symantec.

Symantec Corporation. (2011). *When good backups go bad: Data recovery failures and what to do about it.* Mountain View, CA: Symantec Corporation.

Wallace, M., & Webber, L. (2010). *The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets.* New York, NY: AMACOM - American Management Association.