Volume 15, No. 2
March 2017
ISSN: 1545-679X

INFORMATION SYSTEMS EDUCATION JOURNAL

Special Issue – Teaching Cases

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **EDSIG**, the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is six times per year. The first year of publication was 2003.

ISEDJ is published online (http://isedj.org). Our sister publication, the Proceedings of EDSIGCon (http://www.edsigcon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the 1st Edition of Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for ISEDJ.

2017 AITP Education Special Interest Group (EDSIG) Board of Directors

Leslie J. Waguespack Jr Bentley University President	Jeffry Babb West Texas A&M Vice President	Scott Hunsinger Appalachian State Univ Past President (2014-2016)
Meg Fryling Siena College Director	Lionel Mew University of Richmond Director	Muhammed Miah Southern Univ New Orleans Director
Rachida Parks Quinnipiac University Director	Anthony Serapiglia St. Vincent College Director	Li-Jen Shannon Sam Houston State Univ Director
Jason Sharp Tarleton State University Director	Peter Wu Robert Morris University Director	Lee Freeman Univ. of Michigan - Dearborn JISE Editor

Copyright © 2017 by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to Nita Brooks, Editor, editor@isedj.org.

INFORMATION SYSTEMS EDUCATION JOURNAL

Editors

Jeffry Babb
Senior Editor
West Texas A&M University

Thomas Janicki
Publisher
U of North Carolina Wilmington

Donald Colton
Emeritus Editor
Brigham Young University Hawaii

Cameron Lawrence
Teaching Cases Co-Editor
The University of Montana

Anthony Serapiglia
Teaching Cases Co-Editor
St. Vincent College

Nita Brooks
Associate Editor
Middle Tennessee State Univ

Wendy Ceccucci
Associate Editor
Quinnipiac University

Melinda Korzaan
Associate Editor
Middle Tennessee State Univ

Guido Lang
Associate Editor
Quinnipiac University

George Nezlek
Associate Editor
Univ of Wisconsin - Milwaukee

Samuel Sambasivam
Associate Editor
Azusa Pacific University

2016 ISEDJ Editorial Board

Samuel Abraham
Siena Heights University

Teko Jan Bekkering
Northeastern State University

Ulku Clark
U of North Carolina Wilmington

Jamie Cotler
Siena College

Jeffrey Cummings
U of North Carolina Wilmington

Christopher Davis
U of South Florida St Petersburg

Gerald DeHondt II
Kent State University

Audrey Griffin
Chowan University

Janet Helwig
Dominican University

Scott Hunsinger
Appalachian State University

Mark Jones
Lock Haven University

James Lawler
Pace University

Paul Leidig
Grand Valley State University

Michelle Louch
Duquesne University

Cynthia Martincic
Saint Vincent College

Fortune Mhlanga
Lipscomb University

Muhammed Miah
Southern Univ at New Orleans

Edward Moskal
Saint Peter's University

Monica Parzinger
St. Mary's University

Alan Peslak
Penn State University

Doncho Petkov
Eastern Connecticut State Univ

James Pomykalski
Susquehanna University

Franklyn Prescod
Ryerson University

Bruce Saulnier
Quinnipiac University

Li-Jen Shannon
Sam Houston State University

Jason Sharp
Tarleton State University

Karthikeyan Umapathy
University of North Florida

Leslie Waguespack
Bentley University

Bruce White
Quinnipiac University

Peter Y. Wu
Robert Morris University

Teaching Case

Teaching an Old Dog New Tricks: Disaster Recovery in a Small Business Context

Zach Rossmiller
Zach.Rossmiller@umontana.edu

Cameron Lawrence
Cameron.Lawrence@umontana.edu

Shawn Clouse
Shawn.Clouse@umontana.edu

Clayton Looney
Clay.Looney@umontana.edu

School of Business Administration
The University of Montana
Missoula, MT 59812

Abstract

Many entrepreneurs and small business owners lack disaster recovery plans, which minimize business disruptions caused by failures of critical technical systems. Typically, technology is not the main focus for a small business owner, as most of their time is spent focused on business operations. This case study demonstrates that when a business fails to plan for technological disasters, it can have severe consequences for the business.

In this case, an ambitious and experienced entrepreneur opens a large self-storage facility. The technical systems, which support mission critical elements of the business, were compromised by a power surge and subsequent outage as the result of a major electrical storm.

Part 1 of the case establishes the context as well as the events that led to the failure of critical business systems. Part 2 details how the business recovers from the disaster and the steps necessary to prevent something similar from happening in the future. At the end of the case, the reader will find discussion questions and suggested lab activities that will help students understand the importance of a disaster recovery plan. In addition, students are encouraged to consider implementing a plan to protect their personal data. This case complements the model curriculum objectives in IS 2010.1 and IS 2010.7.

Keywords: Disaster recovery, business continuity, backups, cloud storage, battery backup, case study.

1. INTRODUCTION

Jeff Wolf was a blue-collar entrepreneur who enjoyed building businesses from the ground up. Jeff considered himself a lone wolf with his business ventures because he could never find a partner who matched his energy and dedication to building the enterprise. Once he built a new

venture into a profitable and self-sustaining business, he would often sell the business and move on to a new challenge. Typically, he would sell to a group of employees and maintain a small equity position in the company.

Wolf Storage Solutions, founded in 2008, is a self-storage facility that has a diverse array of storage units ranging from 5 feet by 5 feet all the way to 12 feet by 30 feet. The company differentiates itself from competitors by employing state-of-the-art security systems, which include 16 digital video cameras and a computer-controlled gate access to the facility. The cameras are strategically placed throughout the facility for each customer's security and safety. Of greater importance, Jeff obsesses over customer service. Each of the businesses he founded through the years provided exceptional service to customers.

When Wolf Storage Solutions leases storage space to a new customer a standard process is followed. First, the customer fills out paperwork that captures important information, including the customer's name, billing address and credit card number for recurring monthly billing. Once the paperwork is completed, the information is then transferred into an application management system called Winsen Property Manager, which is a powerful application used to manage every aspect of the business, including site access.

From there, the program generates a unique seven-digit numeric code that is then assigned to each customer. When a customer wants to enter the facility, she is required to enter this unique code into a keypad immediately adjacent to the computer-controlled gate. This also allows the system to monitor the dates and times each customer is in the facility. This information can then be matched up to the digital camera system that is programmed to turn on when motion is detected within the facility.

Finally, the unique code is recorded on the paperwork and a copy is given to the customer. The paperwork is then scanned into a folder located on the computer's desktop. The hardcopy of the completed paperwork is placed in a filing cabinet located in the office.

Although Jeff considered himself a successful businessman and a savvy entrepreneur, he knew that technology was not his strong suit. In fact, he would be the first to admit that he did not understand technology and that he wanted to focus on running the business and not dealing with technical issues.

When he founded Wolf Storage Solutions he hired a "small herd of tech geeks" to install the new system and train he along with his staff on its use. When the system was installed in 2008 it was a state-of-the-art system, but it hasn't been updated since. Unfortunately, the company responsible for the installation has been out of business for several years. To compound the problem, whenever technology-related issues emerged, he usually relied on his part-time employees. Through the years Jeff had a lot of success hiring students from the local university. These employees were all far more comfortable with the technology than Jeff so he often left the technical tasks to them. Unfortunately, the students would often move on after graduation and take along their understanding of the system.

2. THE CALM BEFORE THE STORM

Jeff sipped his coffee and looked out the window. The morning's bright sky had faded into a cold gray by late afternoon. He turned around in his chair and stared blearily at the stack of paperwork on his desk that he would have to tackle tomorrow. When he heard the sound of a car door closing, Jeff stood up and rubbed his eyes. One of his customers walked in just before closing time.

"Hello. How can I help you?" Jeff asked.

"I just need to pay my bill," replied the customer.

Jeff shoved the computer mouse around in a circle to wake the computer from sleep mode and took the customer's credit card.

"It'll take a few minutes. This old thing is taking forever to load," said Jeff as he continued vigorously swirling the mouse on the counter.
"No worries. The weather is starting to get ugly out there," said the customer.

"I heard there was an advisory for high winds and lightning. Hopefully the weather doesn't turn that ugly," chuckled Jeff as he swiped the credit card. "All right, you are good to go unless there is anything else I can help you with today."

At 5 p.m. Jeff locked the front door and exited the office through a door that led directly into the storage facility. A gust of wind nearly blew his hat off as he climbed into his golf cart. He drove around the facility for a general inspection, which involved checking for unlocked storage units or to note when a storage unit appeared to be vacated or damaged. Once he finished the inspection, Jeff

headed back to the office right as it started to rain.

Back inside the office, Jeff opened a closet that housed the system for the facility's security cameras. The system was running with no issues. He was happy with this system. Customers were impressed that the facility was so secure, and the company that installed it also took care of all maintenance and configuration issues.

Jeff ambled back over to the main office computer and shook the mouse to wake the computer again. Jeff opened the Property Manager software and clicked a button called "Business Close" that opened a wizard that took him through the daily closing process. Jeff really liked this aspect of the software because it required everyone to follow the same closing procedures.

The first step confirmed that the auto bill payments will be automatically processed at midnight. The next step confirmed the gate was scheduled to be locked at 10 p.m. Once Jeff received confirmation that the gate has been locked, the last part of the wizard ran a backup of the customer database. The backup of the database was then placed in a folder on the local system labeled "Wolf Storage Backups." When the wizard finished, a green checkmark appeared and then the software switched into "Off-Hours Mode."

3. THE STORM

Sitting in the comfort of his lounge chair at home, Jeff pulled out a remote to turn on his television. He watched the local news report: "Severe thunderstorms and wind in the area. Please be advised." Jeff snorted derisively then took a bite of his dinner. It doesn't take a scientist to tell me that the weather is ugly outside, Jeff thought as the wind howled.

Suddenly, the lights in his house flickered and dimmed, and cracks of lightning lit up the sky and thunder continuously echoed through the valley for the next several hours.

Shortly after midnight, the storm passed. Unbeknownst to Jeff, the damage from the storm crippled his business.

4. THE AFTERMATH

"Most of the power has been restored throughout the city…," announced the radio weatherman. Jeff turned down the volume as he pulled up to Wolf Storage Solutions. He knew the storm had caused some damage in the neighborhood and was anxious to see how his business had fared.

Jeff walked up to the keypad that controlled the main gate and punched in his code. Access denied. *That's odd*, Jeff thought to himself. He tried again, but several beeps and a red flashing light indicated his credentials had been denied. Jeff clenched his teeth as he pulled out his keys and walked up to the office and unlocked the front door. He flipped on the light switch, and the florescent office lights slowly flickered on. *Well, I have power so that's good*, he thought.

He continued to the back door that opened up into the storage facility, got into his golf cart and drove through the facility. He was relieved to find that there hadn't been any physical damage, and all of the rain water drained properly.

Jeff drove back up to the office and went over to the front counter, which housed the main computer, and attempted to wake it from sleep mode by shaking the mouse. No response. Jeff moved the mouse around and hit a few keys on the keyboard. He figured it was just being slow, so he waited a few minutes. Still no response.

Finally, Jeff got down on his knees and opened the cabinet door where the computer tower was located. Because there was no light indication on the front of the tower he pushed the power button to turn on the computer.

"Power must have gone out last night," muttered Jeff to himself as he unplugged the computer and plugged it back in. The computer still would not power on. He decided to check the breaker box to see if the storm tripped a breaker. Jeff stood up and walked into the next room where his breaker box was located on the wall. Jeff opened the panel but did not see any breakers flipped. Jeff tried several more times to turn on the computer, but it still would not power on.

Jeff then picked up his phone to call the only person he knew who could help with a serious technical problem such as this. He called his niece, Stephanie, who graduated from the local university with an MIS degree. Following graduation, she worked for a local consulting firm that specialized in implementing Salesforce CRM systems for clients throughout the country. She was currently working part-time for the local firm while completing her MBA degree. She answered his call immediately, and Jeff explained the situation. Stephanie assured him that it should be an easy fix and that she would be right over.

"How is my favorite niece doing?" Jeff asked her by way of greeting.

"Your *only* niece!" she laughed. "I'm pretty good, but that storm last night caused havoc all over town!"

"I can't believe that it took out my computer system. I had no idea that was possible." Jeff said.

"The other day I read an article about the high percentage of small business owners who do not have any kind of disaster recovery plan or even a basic checklist of steps to take if their technology fails," she said.

"I guess you can say I am one of those business owners. Technology is a foreign language to me," he said.

Smiling wryly at her uncle, Stephanie walked around the counter and opened the cabinet. She pushed the button on the front of the computer and nothing happened.

"Last night, everything was working fine. I went through the closing procedures like I always do at the end of business, then I went home. The wizard in the property management software, was supposed to put the system in "Off-Hours" mode at 10 p.m.," he said.

Stephanie pulled out the computer and placed it on the counter. She tried several different power outlets but the computer still would not turn on. "So this computer plugs directly into the outlet under the counter, right?"

"Yup, that's how the contractors installed it," Jeff replied.

"Because you don't have this plugged into a surge protector or even a battery backup, my guess is that you have a bad power supply."
"Was that something I did?" he asked.

"My guess is the storm last night created some kind of surge and that fried your power supply. It may have fried your motherboard and hard drive, too."

"Is there any way of preventing this?" he asked.
"I always recommend to my clients that they plug their computers directly into a surge protector. This way, it can prevent those voltage spikes," she said.

"I recommend a battery backup to clients who have to have their systems up and running 24 hours a day. Because this computer controls that gate, you should absolutely have this computer plugged into a battery backup. That way, if you have a power outage, your computer can still communicate with the gate for a short amount of time. Power outages usually don't last very long," she said.

"So, what do we need to get my business up and running the right way?" he asked.

"I will run into town and buy a power supply, a surge protector and battery backup. We will start from there and cross our fingers that it is just the power supply. If it is, your computer should be back on in about an hour."

Stephanie returned with the computer parts, opened the computer case and quickly started to untangle the cables. Stephanie wiped away layers of dust. "How old is this computer?" she asked as she replaced the old power supply with the new one.

"I don't know, probably eight years old?" Jeff replied. His niece cringed.

Stephanie finished installing the power supply and turned on the computer. Unfortunately, the computer still would not power on.

Jeff asked her what they should do next.

"Honestly, I think the best idea is to replace this computer with a new one, and I can transfer the data. It will be several hours, but I should have it running this afternoon." Jeff agreed and told her to buy whatever she thought would work best for the business.

Several hours passed and eventually Stephanie walked through the door with a brand new computer.

"So how are you going to get the stuff off of the old computer onto this new one? … Magic?" Jeff asked as she plugged the new computer into the surge protector and battery backup.

"I brought some tools that will allow me to use the old hard drive on your new computer," Stephanie replied as the new computer powered on.

Stephanie clicked through the installation wizard that configured the computer. Once that finished, she pulled out a simple SATA to USB adapter and

plugged the old hard drive into the adapter. She then plugged the USB cable into the new computer thereby connecting the hard drive from the old system to the new computer.
Stephanie patiently waited as the new computer installed the correct drivers. The drivers successfully installed but the old hard drive did not appear. Stephanie placed her hand on the hard drive and realized that the old hard drive was not spinning. It was completely dead. Stephanie turned to her uncle and broke the bad news. "It is not looking good. That storm not only fried the power supply, but it also corrupted your hard drive," she said.

"All of my client information was on that computer— the property management software, the database, everything," Jeff replied.

"What are the chances you have a backup of that database that isn't on the computer?" she asked.

Jeff sighed as he pointed to the filing cabinet labeled "Customer Paperwork." Both Stephanie and Jeff let out a huge sigh as they realized they will have to recreate the database from scratch by manually inputting the original customer paperwork.

"This is going to take weeks of sorting and re-adding the customer data," Jeff groaned.

"It'll be okay. This is exactly the sort of project the company I work for can handle. Let me talk with my boss and see if we can get a small group in here that can get you up and running in the next 24 hours. Be prepared this will cost a few thousand dollars, but it is money well spent," she assured him.

Stephanie called her boss to explain the situation. Her boss was sympathetic and agreed to let her spend the next day or two on this project. In addition, she agreed to send over three MIS student interns from the local university to help.

"Well, Uncle Jeff, help is on the way. It will be about thirty minutes, which will give me plenty of time to install some of the necessary software."

"Excellent! You are definitely a candidate for niece of the year!" he exclaimed.

Stephanie laughed, rolled her eyes and went through the process of setting up the new property management software on the new system.

"I'm going to set this up, and it will look identical to the old interface to you, but I am going to configure a few things differently to prevent this from happening again," Stephanie explained to Jeff.

"First things first, I am going to subscribe you to a service called CrashPlan that will back up your entire computer every night. This will not only back up the computer to an external hard drive, but it will also back up a snapshot of your computer to the cloud. This way, you will have two backups in two separate locations at all times. The daily backup won't interfere with your day to day operations as it will be scheduled to run in the middle of the night," she explained.

"Next, I have subscribed you to another service called Dropbox, which is a cloud service that syncs files between different computers. Each evening when you back up the database as part of the closing procedures it will sync a copy of the database to another computer and provide a backup in the cloud. Basically, you will have two different types of backups in several different locations. If we had this configuration originally, we would be up and running again." Stephanie finished as the fresh-faced interns walked in the door.

After two days of hard work Stephanie and the interns were able to successfully recreate critical parts of the database from the original customer paperwork. Throughout this process, Jeff was busy dealing with upset and concerned customers. If it was not for the original paperwork stored on site and a savvy team of MIS students, Jeff's business would have had major problems.

5. CONCLUSION

For the first time in Jeff Wolf's career he experienced a computer systems failure that brought his business to a standstill. This event compelled Jeff to put more time and attention into the technical aspects of his business ventures. Prior to this event, he didn't put much thought into the technology that was a central component of his business.

In the self-storage business, Jeff had always focused his attention on the physical part of the business as well as providing exceptional customer service. Unfortunately, he neglected a part of his business that many small business owners often neglect – disaster recovery. He realized that almost everything he knew about his customers was mediated and captured via

technology. This critical business asset needed more of his attention.

With Stephanie's help, Jeff implemented a more robust backup system and she helped him develop a written disaster recovery plan that detailed the steps required to help recover the business systems in the event of another major systems failure. Furthermore, she developed a set of simple procedures that could be executed at the end of the week to test the veracity of the backups in the system.

Perhaps of greatest importance, he committed to gain an in-depth understanding of the systems that are critical to his business. He did this by hiring the interns that helped with the data recovery project. He scheduled them for two hours a week for the next three months to teach him about this important part of almost every small business. About halfway through the scheduled sessions he started to see new business opportunities brought about by using more and different types of technology.

Maybe you can teach an old dog new tricks…

6. QUESTIONS AND STUDENT LAB

1. List and describe your "mission-critical" devices that are essential for your school work and daily life.

a) What important data reside on these devices?

b) To what threats are these data vulnerable?

c) Would you be able to recover these data in the event of a catastrophic failure?

d) What steps could you take to protect these data?

2. Identify different types threats that could affect mission-critical systems within businesses. How would you recommend minimizing the impact of each threat?

3. Research CrashPlan and Dropbox. Why do you think Stephanie recommended these solutions? Are both necessary? How does one complement the other? What other technologies are available to achieve the same objectives?

6. Explain how cloud storage services, such as Dropbox, can be beneficial to a small business? What are some potential business vulnerabilities of utilizing cloud storage as the sole means for backing up data?

7. Why is it important to maintain multiple copies of mission-critical data? Why is it important to store copies at geographically separated locations?

8. How often should mission-critical data be backed up? What factors should be considered in timing backups?

Bonus Activities

1. Work with a local small business and perform a risk assessment. If a similar disaster were to befall the business, how would they fare? Help them design a disaster recovery plan. The plan should identify those responsible for recovery of the affected systems. In addition, the plan should provide a detailed overview of the procedures to follow in the event the business was affected by a disaster that compromised the computer systems.

2. Research companies that have experienced a systems failure. What consequences did the system failure have on business operations? What losses were incurred (e.g., data, money, customer loyalty)? In hindsight, what could the companies have done to minimize the severity of system failures?

7. REFERENCES

Beal, V. (2012, October 16). How a Disaster Recovery Plan Can Save Your Business. Small Business Computing. Retrieved from http://www.smallbusinesscomputing.com/tipsforsmallbusiness/how-a-disaster-recovery-plan-can-save-your-business.html

Cerocke, B. (2016, February 24). Create an IT recovery plan to protect against disaster, ransomware. Reno Gazette-Journal. Retrieved from http://www.rgj.com/story/money/business/2016/02/24/create-recovery-plan-protect-against-disaster-ransomware/80868158/

Claims Journal. (2015, September 1). Survey: 75% of Small Businesses Don't Have a Disaster Plan. Claims Journal. Retrieved from http://www.claimsjournal.com/news/national/2015/09/01/265508.htm

CrashPlan Backup. (n.d.). Retrieved from http://www.code42.com/business/

Drew, J. (2012, August 1). Most U.S. small businesses lack disaster-recovery plans. Journal of Accountancy. Retrieved from http://www.journalofaccountancy.com/news/2012/aug/20126135.html

Dropbox. (n.d.). Retrieved from https://www.dropbox.com/

Eckel, E. (2009, February 17). 10 tech mistakes small businesses make (and how IT consultants can help clients avoid them). TechRepublic. Retrieved from http://www.techrepublic.com/blog/10-things/10-tech-mistakes-small-businesses-make-and-how-it-consultants-can-help-clients-avoid-them/

Ekekwe, N. (2011, April 22). Rethink Your Business Continuity Strategy. Harvard Business Review. Retrieved from https://hbr.org/2011/04/refine-your-continuity-strateg

Frenkel, K. A. (2016, April 6). Why Small Businesses Have Big Security Concerns. CIO Insight. Retrieved from http://www.cioinsight.com/security/slideshows/why-small-business-have-big-security-concerns.html

Graham, S. (2015, October 31). Disaster 411: Is your business prepared to fight back? Beta News. Retrieved from http://betanews.com/2015/10/31/disaster-411-is-your-business-prepared-to-fight-back/

IT Disaster Recovery Plan. (n.d.). Ready.Gov. Retrieved from https://www.ready.gov/business/implementation/IT

Parrish, S. (2015, December 28). You're The Most Important Part Of Your Company's Disaster Recovery Plan. Forbes. Retrieved from http://www.forbes.com/sites/steveparrish/2015/12/28/youre-the-most-important-part-of-your-companys-disaster-recovery-plan/#3a37db735c19

Ready.Gov. (n.d.). IT Disaster Recovery Plan. Ready.Gov. Retrieved from https://www.ready.gov/business/implementation/IT

Singh, J. (2016, April 4). De-Fragmenting Disaster Recovery. The Stack. Retrieved from https://thestack.com/cloud/2016/04/04/de-fragmenting-disaster-recovery/

Uninterruptible power supply. (n.d.). Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Uninterruptible_power_supply

Walzer, J. (2009, September 9). Small-Business Guide: Disaster Recovery. The New York Times. Retrieved from http://www.nytimes.com/2009/09/10/business/smallbusiness/10disaster.html