Communications of the IIMA

Volume 5 | Issue 4 Article 2

2005

The Restech Connections CD Project: A Case Study on the Social Construction of Risk

Jason Koch
Northern Illinois University

Jack T. Marchewka
Northern Illinois University

The Restech Connections CD Project: A Case Study on the Social Construction of Risk

Jason Koch
ResTech
Northern Illinois University
DeKalb, Illinois 60115
Phone: 815.753.4008, Email: jkoch1@niu.edu

Jack T. Marchewka
Department of Operations Management & Information Systems
Northern Illinois University
DeKalb, Illinois 60115
Phone: 815.753.1332, Email: jmarchewka@niu.edu

ABSTRACT

Risk management is an important component in understanding and managing information technology (IT) projects. The traditional view of risk management focuses on a three-stage process: identifying risk, assessing risk, and developing a strategy for dealing with each risk. This, unfortunately, may give project stakeholders a false sense of security. Although the application of risk management philosophies, techniques, tools, and methods to managing IT projects is not new, the idea of viewing risk as a social construction outlines a new paradigm for understanding and managing risk. Since the idea of a social construction view of risk has been introduced only recently, no studies have been published to provide support for the development of a theoretical framework. This study provides a case study of an IT project undertaken at a large university located in the midwestern United States. The challenges and problems encountered by the ResTech Helpdesk staff outline a social construction of risk based on not only the organization itself, but also the characteristics of the project, its stakeholders, and other groups involved. Therefore, many of the challenges of this project would be inherent to a university setting but would not be inherent to most other organizations.

Keywords: Case Study, IT Project Risk, Social Construction of Risk

INTRODUCTION

Moving into a college dorm can be an exciting experience. Students meet their new roommates, unpack their belongings, and, of course, plug their computer into the high-speed connection in their room. Then something unusual happens: Within minutes after a student powers on his or her computer, it becomes compromised by a virus and turns into a "bot" that sends hundreds of spam emails or strikes corporate servers with a denial of service (DOS) attack. Moreover, a student's computer now becomes so busy with these new activities that it now performs simple tasks at mind-numbingly slow speeds.

Computer virus and spyware affect everyone; however, a college network may be more susceptible than most corporate networks in terms of the variety and velocity of attacks. This problem stems from two issues. First, most universities insist upon an "open" network in order to facilitate communication and learning. This usually entails inadequate firewall protection to prevent malicious traffic from entering (or leaving) the network. This lack of basic defense makes college networks an enticing target for attacks and a breeding ground for new viruses. Therefore, the strategy often used follows that if you can't protect the network, just protect the machines connected to it.

The second, and more serious issue, relates to the eclectic collection of student-owned technology. Often the collection of technology include every type and brand of computer sold in the last ten years with a myriad of software packages from different vendors. While the cadre of students today is increasingly viewed as tech-savvy, many have inadequate knowledge of computer security. Current desktop software has done much to "shield" end users from the complexities of computers.

One way for frustrated IT staff to combat this problem is to educate the users. There are some basic things that users can do to protect themselves from attacks. The most basic is to keep the operating system up-to-date with the most current patches, installing antivirus software, and following some "safe computing" practices such as not opening unknown email attachments. The challenge then becomes how to communicate this information to thousands of students every semester.

This paper provides a case study of a project called the ResTech Connections CD. This project was undertaken by a large, Midwestern university in order to overcome many of these problems. Many of these challenges encountered during the project could be viewed in terms of a traditional risk management approach; however, since many of these issues are largely determined by the nature of the institution in terms of its culture, policies and procedures, and even by the nature and choice of projects undertaken, a social construction view can be taken. The nature of risks, decisions, and outcomes of this project suggest that the case study is a valid approach for understanding the complex interrelationships that exist among these dimensions (Stake, 1995).

The remainder of this paper will include three main sections. In the first section, the background for the project will be introduced. This section will provide an overview of the project and describe many of the challenges encountered by the ResTech Help Desk staff. An analysis of the actions and decisions made will follow in the next section. Finally, the last section of this paper will provide a discussion of some lessons learned and how a social construction view of risk can be applied to this project.

BACKGROUND

The ResTech Helpdesk

The ResTech Helpdesk was formed in 1997 by Student Housing and Dining Services (SHDS) at a large Midwestern university with the mission to provide technical support for students living in the residence halls. Currently, the Helpdesk employs approximately twenty part-time student workers, one full-time manager and a graduate assistant. Most of the students are computer science majors who begin working in their sophomore year and stay until they graduate. The Helpdesk is responsible for first-line support for about 6,500 residents and 300 staff members. In addition to phone and on-site support, it offers free in-house hardware and software repairs or upgrades. The information used in the preparation of this case was acquired from interviews with the Helpdesk Manager as well as the various staff members who were directly involved in the project.

The Connections CD Project

There are different methods for delivering high-speed internet access to the University's residence halls. Some use DSL and require an external modem to be connected to the phone jack, while others have a single Ethernet port in the room. Students who share a dorm room often set up a hub so each roommate can share a single connection. The proper equipment is in the room when students arrive, but setting it up correctly has always been a challenge. In most rooms there are multiple jacks, none of which are labeled, and only one of which is active.

Over 5,000 students typically move into their dorm rooms on a single day before the beginning of each semester. Many students with computers attempt to connect their computer to the network, become frustrated, and then call the Helpdesk. The Helpdesk has four phones so high student demand becomes problematic. On average, it takes about ten minutes to walk a student through the set up their computer equipment over the phone. However, this may take much longer if settings on the computer need to be changed or if parents try to be "helpful." ResTech quickly realized the need for a better way of instructing students on how to setup their equipment.

Initially, the ResTech staff placed a flyer in each room with some crudely-drawn pictures and step-by-step instructions. This had almost no effect on the volume of calls the Helpdesk received. Fortunately, ResTech had a student skilled in Photoshop, and he suggested that they create instructions with digital pictures, arrows, and highlighting of important instructions. It was considered a much better idea and it wasn't long before someone suggested that this information could be delivered on a CD.

Subsequently, the first Connections CD included a collection of web pages that could walk the user through the network access process. The user could choose whether they had a DSL or Ethernet connection, and a page with pictures would display instructions on how to set it up. In addition, it provided instructions on how to configure a computer's network settings. Overall, the consensus was that this approach worked fairly well. When a student

called the Helpdesk with a question, they were instructed to use the Connections CD and then call back if they still had problems making the connection. However, many people had issues figuring out what type of connection they had and some just could not understand the pictures.

Over the next two years, the Connections CD was updated with new pictures and instructions for new operating systems, as well as additional features like campus information and links to helpful websites. Despite this effort, the pictures and instructions on the CD continued to bewilder many students. At the same time, ResTech witnessed a large and growing increase in the number of virus infections to the point where the Helpdesk staff was spending more time cleaning them up than any other type of support. Again, it became apparent that the Helpdesk needed a better tool to support its user community.

Project Goals

A project to create a new version of the Connections CD had two goals: First, develop better instructions for equipment setup and, second, provide students with a tool to keep unprotected machines off the network until they could be secured.

To achieve the first goal, ResTech had several new tools at their disposal. The skills of some of the Helpdesk employees now included web scripting and, more importantly, digital video editing. The combination of the two meant that a student could choose where they lived (i.e., not what type of connection they have) and then watch a video with sound and special effects to walk the user through each step in the network access process. Through multimedia, ResTech could deliver a customized solution for a given residence hall and connection type.

The second goal was a bit more challenging because students would have to access the network first in order to download the most current software patches. This presented a risk in that a machine could be infected before the appropriate security patches could be downloaded and installed. However, the ResTech staff believed that they had come up with a good solution. Luckily, the Helpdesk staff had developed several programs or batch files for many of its in-house computers that could identify a computer's operating system and then apply the appropriate patches automatically. It was reasoned that if ResTech gave these tools to the students on the Connections CD, then each student could then run the program to secure their machine from major exploits without connecting to the network in order to download the required patches.

In response to the growing virus threat, the University had previously purchased a volume license from MacAfee that would allow any student living in the residence halls to have free use of this antivirus software. The Helpdesk was already installing this software on all of the machines that came into the office to be fixed, so the install program was simplified so that the user was not required to provide any input. They would just have to double-click on an icon to open the program and then reboot their computer after the program finished. It seemed, therefore, logical to include this set of programs on the new Connections CD as well.

Lastly, the Helpdesk employees often came across free tools that could be downloaded and used to clean and secure machines from viruses and spyware. These included scanning and removal programs, alternate web browsers, and sites with information concerning new security threats. Because these programs are frequently changed and upgraded, it was decided to include only links to these various software packages on the Connections CD. In addition, ResTech included information about each program's purpose and reason for use. The idea was to educate students on tools they could use to defend themselves against computer-related security threats.

The Project Schedule and Budget

There was no formal schedule or budget for this project. In fact, there was probably nothing formal about this project at all. That's just the way most things are done at the Helpdesk. There is a very informal atmosphere and most of the employees do not have to worry about much other than arriving to work on time. There were no formal roles on this project; if a person had the skills to complete the task, they did it. Because the Helpdesk is not responsible for generating revenue, they generally do not worry about how costs are allocated.

For example, the schedule was nothing more than a deadline. After talking to a printer, the staff knew that they had to have the final copies of all materials no later than August 1st if they wanted to have adequate time to distribute copies of the Connections CD to the residence halls before fall move-in day. In addition, the Helpdesk was often too busy to start working on many of its projects until the start of summer break when the demand for student support is at its lowest. In short, this meant that the project had to be completed in approximately ten weeks.

The Helpdesk budgets for a certain number of hours to be worked each week over the break. The cost of these hours is determined by taking the average pay rate of all the Helpdesk student employees. They do not keep track of the amount of time a person spends on a specific project - they just try to do everything they can with the people who are there at the time. Therefore, there was no discernable way to estimate the number of hours spent on the Connections CD or the associated cost. In short, only two direct costs that could be traced to the project: A digital video camera used to make the videos ($700) and the cost of printing the CDs ($2,500).

The Project Stakeholders

One thing that has made the Helpdesk effective is that all employees are encouraged to contribute ideas and participate actively. New ideas are frequently suggested to management, and employees are then given the opportunity to try out these ideas. Each year the CD is updated and just about everyone has a suggestion for something to be changed or added. Those with the most ideas or relevant skills are picked to work on the project, but in the end it appears that most everyone has contributed. The particular appeal of this project is that employees use it almost everyday while supporting students. This makes everyone a stakeholder as a better CD would make their jobs that much easier.

The person ultimately responsible for the completion of the project is the Helpdesk Manager. His responsibility is to make sure the student workers stay on task and have the tools they need to complete the project. Specific development decisions were usually made by the Manager along with the students working on the project.

Project Challenges

The initial stages of the project went smoothly. The basic scripts were written to control the user's path though the CD and the basic layout of pages was decided on. However as the specific goals of the project were becoming clearer, the team encountered several problems and challenges.

The first function put on the Connections CD was an auto-patching system. This appeared to be a good choice because it was already complete and just needed to be copied onto the CD. Luckily, management thought to ask the campus-licensing department if it was legal to include Microsoft patches on the Connections CD. As it turns out, Microsoft considers it illegal for any other party to distribute their patches, even though they are available free if downloaded. Microsoft, however, offered to provide the University with their own CD's full of updates for $20 a copy.

Not surprisingly, the decision was made not to include the updates on the CD, but rather to include links to the Microsoft update website. Unfortunately, all the work had already been completed by the time that the Helpdesk staff found out that they could not include the patches on the Connections CD. This feature now had to be scrapped and a new page was created to explain how to download the patches from Microsoft's Web site. This also meant that students would have to connect to the network to download the patches, and possibly have their computers become infected before the security patches could be applied.

In an effort to track the number of licenses given out, ResTech was also told that they could not put the antivirus software on the disc. Students would be required to go to a web page where they would have to log in before downloading the software. These two changes made the CD essentially useless in preventing users from connecting unprotected machines to the network. Thus, without any help from the people directly involved, the project was doomed to fail in achieving one of its goals.

However, a dark cloud often has a silver lining, and there was still some hope of protecting students from the network. The Helpdesk staff was informed by Information Technology Services (ITS) – a centralized IT department for the university – that they were developing a system that would block students from the network until their computer had been registered and several required security patches were installed. This system would allow ITS to identify and disable any user' computer that contracted a virus. ITS promised that this system would keep users safe from attacks until their machines could be protected, and they promised that the system would be available before fall move-in day.

This was good news; unfortunately, it created a new issue. The basic idea of the CD was to take a student though each step of the physical setup in order to configure their computer and connect to the Internet. Now the staff was being told that there would be one additional step, registering the machine, before a student could access the

Internet. Obviously, it would be important to include this step on the Connections CD, or students would be lost when they reached this final step. ITS had no firm idea as to what that final step would involve, but they promised to provide updates as development of the system continued.

Meanwhile, efforts were focused on shooting the videos for the step-by-step instructions for each type of setup. During this time, another problem was discovered. There was only one student working over the summer with experience in video editing. In addition, this person took a series of unannounced vacations around the end of June. It did not appear to be an issue at the time because there was no detailed schedule. It was believe that everything would be fine as long as everything was completed by August 1st.

Consequently, the rest of the staff found it difficult to design documentation around videos if they didn't know how many videos there would be, what each would cover, or even the length of the video. These decisions were left to the student in charge of producing the videos (i.e., the one that was on vacation and then only worked 10 hours a week when he was there). Progress ground quickly to a halt.

Over the last month of the project, many changes were made, many long nights were worked, and a many insults and objects were thrown. Somehow, the project's scope was completed and only a week late. Only the one last piece of the puzzle remained: ITS needed to provide the process for registering the students' computers. It was decided to create a web link at the end of the configuration process and tell the student that they would need to complete it before they could get online. ITS gave assurances that they would have a Web page ready to take the student thought the rest of the process.

About a week before move-in day, the HelpDesk staff met with ITS. ITS explained that despite buying some very expensive hardware and having several engineers working on the system for most of the summer, they could not get it to work. Therefore, that last "Get online" link on the Connections CD would point to a page saying "Congratulations! You're online!" even though the students were not.

ANALYSIS

The Helpdesk staff was given ample time and resources to complete this project. The goal of the project was well defined and many of the people involved even had experience working on pervious versions. The crux of the problem that plagued this project was a lack of a project management methodology. The funny (or sad) thing is that similar problems occurred during the development of previous version and in other projects undertaken by the Helpdesk.

The main issue was the lack of any type of project schedule. The tasks required to complete the project were not defined, and consequently no one knew when a particular task should have been started. Add to this a lack of any formal roles and it creates a serious weakness. An employee who is working on multiple projects is likely to focus on the project or tasks that appear most urgent while neglecting others that may need to be completed before the project can proceed.

Another major issue was scope change. Employees frequently started working on a feature they felt was important, only to find out later that is wasn't feasible. This problem stemmed from a lack of process to evaluate the costs and benefits of a change. In addition, most of the student workers did not understand the full impact of some of their decisions, such as the legal implications of delivering patches on CDs. Changes should have been approved by members of management before the work started. As a result, a great deal of time was lost pursuing abandoned ideas.

The lack of a project methodology is partly due to time constraints. The Helpdesk had been growing very quickly over the last few years and was responsible for more work with almost the same level of staff. Moreover, managers did not have the time they would like to spend with each project. The general feeling about projects was to work as hard as you can and somehow they would get done.

DISCUSSION

If this project had had a detailed schedule, some of the problems involving "missing" staff could have been foreseen and possibly avoided. If the Helpdesk's management had been more concerned with the schedule and not just deadlines, they could have saved money and minimized stress. Creating a schedule could also have helped in managing other projects that seemed to overextend the current staff.

More than anything else, the lessons and experience gained from this project suggest that management cannot leave a project team to their own devices and expect them to be successful. This team was very skilled and motivated, but the project was late, over-budget, and failed to attain one of its main goals. There has to be a project manager present to enforce a methodology on the group, in order to prevent problems like the ones that occurred in this project.

In addition, effective managers have the responsibility to learn from past projects and mistakes in order to adapt the methodology to fit the organization. As mentioned previously, this project suffered from many of the same problems that occurred on previous versions of the Connections CD. Someone could have taken the time to look at each version after it was completed to identify what was done wrong and what could be done next time to make sure it doesn't happen again. If not, managers are doomed to repeat these mistakes.

As a side note, the Connections CD 3.0 has been a useful tool for the Helpdesk. The Helpdesk's policy when someone calls with connection problems is to tell them to go through the Connections CD and then call back if they still have problems. Callbacks are now rare. The consensus of the Helpdesk staff today is that this is an example of a project that failed, but still managed to create something useful.

In conclusion, this study provides an opportunity to view project risk from a social construction view. As Carsten Stahl, Lichtenstein, and Mangan (2003) contend, the traditional approach to risk management is based on a flawed assumption that risk can be viewed objectively. The traditional view of risk management focuses on risk identification, risk assessment, and then developing a strategy for dealing with each risk identified (Smith, McKeen, & Staples, 2001). The information systems literature has included a number studies that have advocated traditional risk management approaches and techniques for improving the likelihood of IT project success (Alter & Ginzberg, 1978; Barki, Rivard, & Talbot, 1993; Boehm, 1991; Marchewka & Keil, 1995; McFarlan, 1982). In addition, Keil, Tiwana, and Bush (2002) have identified a number of risk factors or conditions that pose a threat to the success of the IT project. Subsequently, this may give the project manager, the project team, or other project stakeholders a false sense of security that risks can be identified and dealt with effectively. Casten, Stahl, Lictenstein, and Mangan (2003) suggest that since risk is a social construct, stakeholders should engage in discourse concerning the nature and evaluation of risk. More specifically, risks should be assessed in terms of their context or relation within specific projects. This includes not only the organization itself, but also the characteristics of the project, its stakeholders, and other groups involved. Therefore, many of the challenges of this project would be inherent to a university setting but would not be inherent to a for-profit organization. For example, the culture of ResTech is primarily preordained by the culture of the University and the fact that student workers make up the bulk of the Helpdesk staff. Although these traits may be inherent to a university, they most likely would not be found in say a healthcare organization. The commonality of a relatively inexperienced staff, lack of formal project management processes and controls, and management structure largely determine the social construct for understanding the risks and subsequent challenges associated with this project.

This paper provides perhaps a second step in developing an understanding a social construction view of risk. While Carsten Stahl, Lichtenstein, and Mangan (2003) introduced this interesting and novel idea, this paper provides a backdrop for continued discussion for understanding and applying this new view. Moreover, it is hoped that this will encourage others to view risk as a social construction so theoretical frameworks can be developed and tested in future studies.

REFERENCES

Alter, Steven & Ginzberg, M. (1978) Managing uncertainty in MIS implementation. *Sloan Management Review*, 20, 23-31.

Barki, H., Rivard, S., & Talbot, J (1993): Toward an Assessment of Software Development Risk. *Journal of Management Information Systems*, 10(2): 203-225.

Boehm, B (1991): Software risk management, principles and practices. *IEEE Software*, January, 32 - 41

Carsten Stahl, B., Lichtenstein, Y., & Mangan, A. (2003). The limits of risk management: A social construction approach. *Communications of the IIMA*, 3, (3). 15-21.

Keil, M., Tiwana, A., & Bush, A. (2002) Reconciling user and project manager perceptions of IT project risk: a Delphi study. *Information Systems Journal* (12): 103 - 119

McFarlan, F.W. (1981). Portfolio approach to information systems. *Harvard Business Review*, 59(5): 142-150.

Marchewka, J.T., & Keil, M. (1995). A portfolio theory approach for selecting and managing IT projects. *Information Resources Management Journal.* 8, 5-14.

Smith, H.A., McKeen, J.D., Staples, D.S. (2001). Risk management in information systems: Problems and potentials. *Communications of the ACM*, 7.

Stake, R.E. (1995). *The art of case study research.* Sage Publications, Inc., Thousand Oks, CA.