Communications of the IIMA

Volume 10 | Issue 2 Article 1

2010

The FBI Virtual Case File: A Case Study

Jack T. Marchewka
Northern Illinois University

The FBI Virtual Case File: A Case Study

Jack T. Marchewka
Northern Illinois University
jmarchewka@niu.edu

ABSTRACT

The Federal Bureau of Investigation (FBI) began developing a case management software system called the Virtual Case File in 2000, but eventually abandoned the project in April 2005. The cost of this project was estimated to be over $170 million, and this waste of tax payer money drew sharp criticism. The impetus for the project was due to the FBI's aging technology infrastructure that included 386-based personal computers and a 12-year-old network system. In 2000, Congress allocated almost $340 million for the proposed FBI Information Technology Upgrade Project (FITUP) that was soon divided into three parts and renamed Trilogy. This project was scheduled to take three years and included an enterprise-wide upgrade of desktop hardware and software and the implementation of a more modern and secure network. In addition, a Virtual Case File system would include a case management system, an evidence management system, and a records management system that would replace the FBI's antiquated case management system which limited the FBI's ability to carry out its mission effectively. This study provides a qualitative analysis of this IT project failure. More specifically, this study attempts to answer the questions: Was the failure of the FBI's Virtual Case File project unique? Or does it share common characteristics with other IT project failures? This case study should be of interest to IT academics in terms of teaching project management or as a theoretical basis for guiding future research. This study should also be of interest to IT practitioners in terms of understanding some important project management challenges when attempting to implement an IT solution.

INTRODUCTION

Managing information technology (IT) projects continues to be an ongoing challenge for many organizations worldwide. For example, a survey conducted by the Standish Group (1995) called CHAOS drew attention to what many called the software crisis when it reported that only 16 percent of the application development projects were successful in terms of being completed on time and within budget. Moreover, about 31 percent of the projects were canceled before completion, while 53 percent were completed but over budget, over schedule, and not meeting original specifications. The average cost overrun for a medium-size company surveyed was about 182 percent of the original estimate, while the average schedule overrun was about 202 percent. That is, the results of the survey suggest that a medium-size project estimated to cost about $1 million and take a year to develop actually cost about $1.8 million, took just over two years to complete, and only included about 65 percent of the envisioned features and functions.

However, the original CHAOS study published in 1994 was the first of several studies conducted every two years by the Standish Group. Figure 1 provides a summary of the CHAOS studies conducted from 1994 through 2006. Although, in general, it appears that the percentage of

successful projects is increasing, a large percentage of challenged and unsuccessful projects suggest that there is ample opportunity for improving project performance.

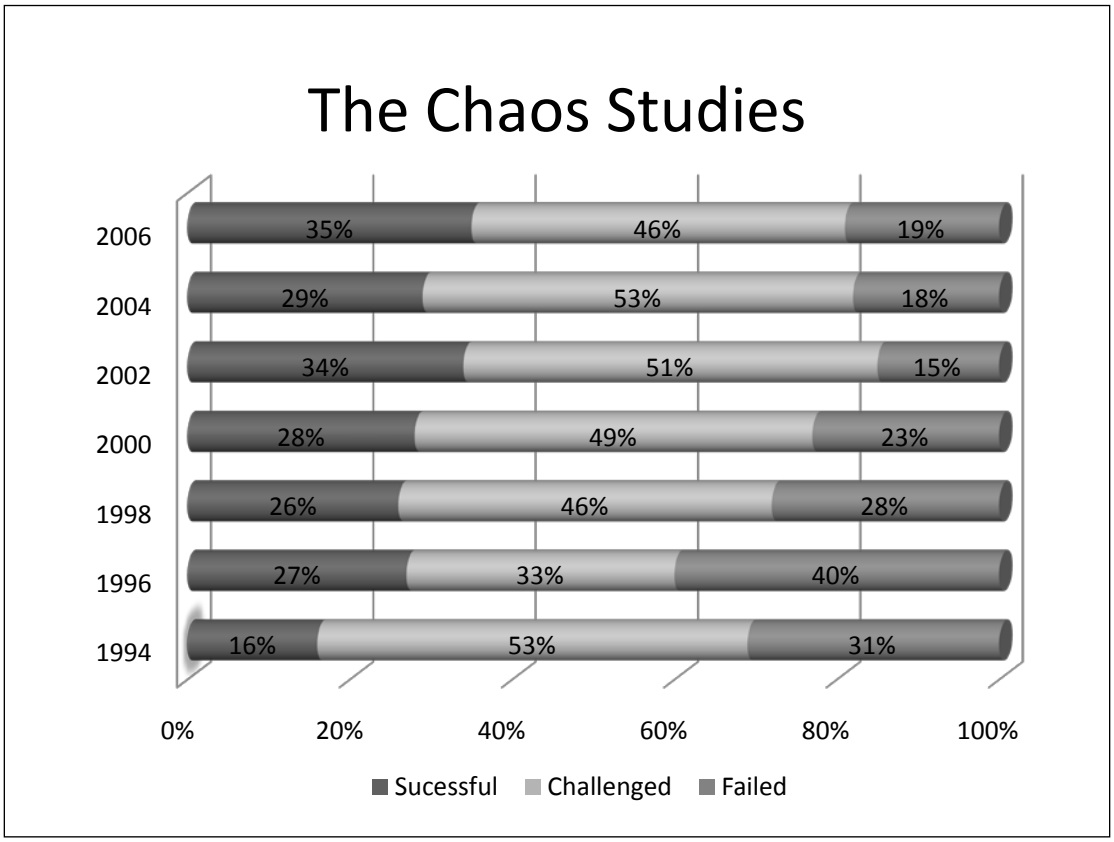

Figure 1: Summary of Chaos Studies from 1994 to 2006 (Marchewka, 2009).

While the CHAOS studies focused on IT projects in the U.S., a study of 800 senior IT managers from the U.K., United States, France, Germany, India, Japan and Singapore conducted by Tata Consultancy Services (2007) provides a more global view and reports dire results similar to the CHAOS studies:

- 62% of the IT projects failed to meet their schedules
- 49% experienced budget overruns
- 47% experienced higher than expected maintenance costs
- 41% failed to deliver the expected business value and return on investment (ROI)

It appears that there is ample opportunity and a need to improve the likelihood of IT project success. Therefore, the purpose of this study is to provide a rich qualitative analysis of the challenges and decisions that led to the failure of a major U.S. government project. Subsequently, the information and data collected for this study was available from a number of public sources because project failures involving public money are documented (Al Neimat, 2005). The research question is whether this project failure was unique or did it share

characteristics with other failed IT projects. This can be accomplished by conducting a case study of the FBI's failed Virtual Case File (VCF) project and comparing the findings to several empirical surveys of failed IT projects. This may provide valuable insight as to why particular projects fail and how certain events or decision may increase the likelihood of failure.

In general, a case study provides an appropriate research strategy when "how" or "why" questions are of primary interest, when the researcher does not have significant control over events, or when the phenomenon of interest takes place within some real-life context (Yin, 1994). Moreover, descriptive or qualitative research may be undertaken when description and explanation are of greater interest than prediction (Merriam, 1988).

This study should be of interest to IT practitioners in terms of understanding some important project management challenges when attempting to implement an IT solution. Moreover, this case study should also be of interest to IT academics in terms of teaching project management or as a theoretical basis for guiding future research. Taken together, this may help increase the likelihood of IT project success.

THE VIRTUAL CASE FILE PROJECT

The Trilogy Project

After years of developing information systems without an overarching organizational view, the FBI found itself with an "improvised" IT infrastructure with more than 50 independent application systems written in different programming languages and running on disparate platforms (Verton, 2003). In September 2000, Congress approved $379.8 million for a three year project that was called the FBI Information Technology Upgrade project under the direction of FBI Director Louis Freeh. At this time, the FBI did not have a CIO, documentation of its current systems, or a plan for renovating them (Goldstein, 2005).

However, the FBI Information Technology Upgrade project was eventually divided into three parts and renamed Trilogy. The Trilogy project centered on upgrading the agency's 56 field offices and 22,000 agents and support staff with new desktops and servers, Web-enabling a number of the most important investigative database systems, and, most importantly, a Virtual Case File (VCF) system that would automate the antiquated paper-based Automated Case Support (ACS) system (Goldstein, 2005).

The VCF was envisioned to help FBI agents efficiently share data about cases in progress, especially terrorist investigations. The system would also enable agents anywhere in the United State quickly to search various documents and allow them to connect possible leads from different sources. In addition, the VCF would include a case management system, an evidence management system, and a records management system. The intention was to eliminate the need for FBI employees to scan hard-copy documents into computer files. A custom-developed system was needed since no existing commercial software packages were available that meet the agency's needs when the project began in 2001. In the spring of 2001, development of the VCF software was contracted to Science Applications International Corp. (SAIC) in San Diego, California and was to be completed by late 2003 (Rosencrance, 2005).

Post 9/11

In September 2001, one week before the 9/11 terrorist attacks, Robert Mueller replaced Louis Freeh as the director of the FBI. The terrorist attacks laid bare the inadequacies of the FBI's information systems (Goldstein, 2005). The FBI concluded that it was losing intelligence as fast as it could gather it (Eggen & Witte, 2006).

Due to intense public and congressional pressure, Mueller instructed that the three year schedule be put into overdrive so that the Trilogy project could be completed "as soon as technically possible" (Verton, 2003). A few weeks after the September 11th attacks, Robert Chiaradio, an agent in charge of the field office in Tampa, Florida, was hired by Mueller as an executive assistant director of administration.

Following a number of discussions with Mueller, Chiaradio believed that the current plans for just adding a Web interface on the ACS system was not going to provide value to the FBI agents who would use the system. To help him out, Chiaradio brought in Special Agent Larry Depew who was known as a "G-man's Gman" in October 2001 (Goldstein, 2005). In the early 1990s, Depew had developed a database system on his own to track Russian and Mafia mobsters in New Jersey. After reviewing and recognizing the limitations of the Web front end for the ACS system, Chiaradio and Depew convinced Mueller that the FBI needed an entirely new system with an improved user interface and database management system that could store millions of records and allow agents to analyze "relationships on everything from witnesses, suspects, and informants, to evidence such as documents, photos, and audio recordings" (Goldstein, 2005). In December 2001, SAIC was told to stop building a Web front end to the FBI's existing systems and instead begin development of a new application to replace the old ACS.

With increasing internal and external pressure to get this system in the hands of the agents, Depew proceeded to take a more "cavalier" approach to systems development by taking a number of shortcuts in terms of planning or developing a blueprint that would guide critical decisions. According to Depew, his development team began "to feel our way in the dark" as no guidelines or documentation mapped the FBI's processes and IT infrastructure (Goldstein, 2005).

Depew's team held a series of Joint Application Development (JAD) sessions with SAIC engineers, and other experts to define the requirements for the new VCF system. SAIC and the FBI committed themselves to creating a new case management system in 22 months that would replace the existing ACS using a risky implementation strategy called flash cutover. Essentially, the agents would log off from ACS before going home from work in the afternoon and then log on to the new system the next morning. There would be no going back or backup plan if the new system didn't work (Goldstein, 2005).

In January 2002, the FBI requested an additional $70 million from Congress to accelerate the Trilogy project, but received $78 million. SAIC agreed to deliver the VCF system in December 2003 rather than June 2004. To expedite development, SAIC split its VCF development teams into eight groups so that they could work in parallel on different components of the system. As Rich Reynolds, vice president of SAIC, said, "People forget the urgency that we were under and

our customer was under. And we were right beside them. We were in the foxhole together" (Goldstein, 2005).

While Depew's team communicated the FBI's investigative and administrative processes to the SAIC engineers, Mueller and Chiaradio hired C. Z. (Sherry) Higgins, a seasoned IT professional, to create the Office of Program Management. Higgins would be in charge of centralizing IT management and overseeing the FBI's most expensive, complex, and risky projects, as well as manage Trilogy. One of her first decisions was to name Depew, who had no IT project management experience, the VCF project manager (Goldstein, 2005).

By mid-April, it became apparent that the vendor contracted to deliver the workstations and network would not meet the July schedule. Meanwhile the six months of exhaustive JAD sessions produced a very detailed requirements document. The requirements called for combing the ACS system with the FBI's central repository of investigative telephone records and another repository for investigative data about people, organizations, locations, vehicles, and communications. In addition, the VCF would store scanned documents, photographs, and other electronic media for evidence tracking. This would change how work flowed through the bureau dramatically as agents would complete forms online and then route them to the appropriate supervisor's inbox. The agent would then be able to track it to see whether it had been approved (Goldstein, 2005).

After 18 months, Robert Chiaradio left the FBI to take a new position as managing director of homeland security at BearingPoint Inc. in McLean, Virginia. By the summer of 2002, SAIC had approximately 200 programmers and was looking to add more people. Matthew Patton was hired as part of the security team which reviewed the design documents describing VCF's overall structure, logic, and user interface. Patton held a B.S. in information and decision systems from Carnegie Mellon University and served as a cadet in the U.S. Air Force Reserve Officers' Training Corps. He also had spent four years of military duty in the Office of Secretary of Defense in the Pentagon where he helped develop a Web-based database system used to plan the Department of Defense's $400 million budget (Goldstein, 2005).

Blowing the Whistle

Patton soon realized that SAIC was not interested in his opinions and was told "not to rock the boat" when he began expressing his concerns regarding potential security and design issues. As he stated, "They were trying to design the system layout and then the whole application logic before they had actually even figured out what they wanted the system to do" (Goldstein, 2005). For example, Patton argued that the 800-plus pages of requirements were too bloated and complicated.

In addition, Patton complained that SAIC made no attempts to control costs with the 200 programmers who were on staff to "make work" when only a couple of dozen would have been sufficient. Patton pointed out, "The company's attitude was that it's other people's money, so they'll burn it every which way they want to" (Eggen & Witte, 2006).

Patton also claimed that SAIC attempted to write much of the VCF code when an off-the-shelf product like Novell's Groupwise email system was already being used by the FBI and would have been more appropriate to use than coding a new email application from scratch. Patton was told to "calm down and be a team player (Goldstein, 2005). Out of frustration, Patton posted a message to InfoSec News that mentioned he was working on the Trilogy case management system and that no one was taking security issues seriously. In his posting, he asked for help getting in touch with someone at the FBI who would care and demand accountability from its contractors. He ended with the question: "Shouldn't someone care?" (Goldstein, 2005).

However, Sherry Higgins saw the message and reported Patton to the FBI's security division, where he was questioned about breaching national security and his top secret clearance. Higgins called Patton a disgruntled employee who posted inaccurate and sensitive information (Goldstein, 2005). Patton's security clearance was revoked. Unable to continue working on the project, he ended up leaving his programming job three months after posting his concerns (Eggen & Witte, 2006). Also at this time, the FBI and SAIC agreed to a baseline set of requirements so that SAIC could begin development (Goldstein, 2005).

More Funds Needed

By December 2002, the Trilogy project was in need of additional funds, so Higgins asked Congress for an additional $137.9 million. However, the inspector general issued a report that described "… a lack of critical IT investment management processes for Trilogy contributed to missed milestones and led to uncertainties about cost, schedule, and technical goals" (Goldstein, 2005). Undeterred, Congress approved another $123.2 million which now increased the total cost of the project to $581 million.

SAIC programmers continued to work on the project, and the decision was made to use a spiral development approach. However, approximately 400 change requests were filed in 2003. Although some of these requests were minor, some had a major impact. For example, after about 25 percent of the code had been written, the FBI requested a "page crumb" feature inspired by the fairly tale of Hansel and Gretel that would allow users to identify the path taken while navigating through various screens. According to Reynolds at SAIC, "Once they saw the product of the code we wrote, then they would say, 'Oh, we've got to change this. This isn't what I meant. And that's when we started logging change request after change request after change request" (Goldstein, 2005).

Tensions between SAIC developers and the FBI increased over the winter and spring of 2003. In addition, the vendor contracted to deliver the workstations and network informed Higgins that delivery would be delayed until October, but that eventually became April 2004. Although installation of the workstations began in 2001, problems involved changing email systems from Novell's Groupwise to Microsoft Outlook and acquiring components to connect the individual field offices to the wide area network. These problems were compounded by the FBI's sloppy inventories of existing networks and an underestimation of how bringing all 22,000 users online at the same time would strain the network (Goldstein, 2005).

In September 2003 the Government Accountability Office (formerly the U.S. General Accounting Office) issued a report that warned that the FBI was exposing its modernization efforts to undue risk because it was working without an enterprise architecture (Grimes, 2005). According to Randolph C. Hite, who worked for the GAO, "It was a classic case of not getting the requirements sufficiently defined in terms of completeness and correctness from the beginning. And so it required a continuous redefinition of requirements that had a cascading effect on what had already been designed and produced. Had there been an architecture, the likelihood of these requirements problems would have been vastly diminished" (Goldstein, 2005).

The VCF project and problems continued as SAIC began testing the system in the fall of 2003. In December, Zalmai Azmi was named the acting CIO for the FBI, and SAIC delivered the VCF to the FBI. Azmi made the decision to reject delivery, and the FBI documented 17 functional deficiencies that SAIC would have to fix before the system would be accepted. SAIC argued that many of these deficiencies were requirements changes, so an arbitrator was called in. In March 2004, the arbitrator released a report that found fault with both the FBI and SAIC. According to the report, 59 issues and sub-issues were derived from the original 17 deficiencies – 19 were due to requirements changes and the FBI's fault, while the remaining 40 were SAIC problems. SAIC offered to make all the changes if given one more year and $56 million. Azmi rejected the offer (Goldstein, 2005).

Unfortunately, this did not seal the VCF project's fate. SAIC continued to fix coding errors, while Depew's team developed investigative scenarios that could be tested on the system. In fact, Mueller provided an optimistic testimony to a Senate subcommittee that VCF would be operational by the summer of 2004. According to the *Washington Post*, Mueller testified that the FBI experienced a delay with a contractor and that the problems had been solved. Moreover, he expected that the VCF would be delivered by summer (Eggen & Witte, 2006).

In May 2004, Azmi was officially named the FBI's CIO. In June, the FBI contracted with Aerospace Corp. as an independent reviewer to assess whether the system requirements were accurate and complete. In addition, Azmi requested SAIC to change an electronic workflow function of the VCF system into something called the Initial Operating Capability (IOC) for a fixed price of $16.4 million. The schedule would be six months and IOC would be delivered to almost 500 field personnel in the New Orleans and Baton Rouge field offices, as well as a drug enforcement unit in the Hoover Building. This also led to a change of managers as Rick Reynolds at SAIC replaced Brice Zimmerman, while Depew left to become the director the FBI's New Jersey Regional Computer Forensics Laboratory. In addition, Sherry Higgins quit her position at the FBI and moved back to Georgia before the IOC project was launched. In her view, "When it's not fun anymore, Sherry's not a happy girl. The writing was on the wall that IOC was going to be Zal's project. And I just felt like it would be better for me and Zal for me to leave" (Goldstein, 2005).

Unlike his three predecessors, Azmi was involved in the day-to-day operations of the new IOC project. As of June 2004, SAIC had about 120 of its engineers working on the IOC project, but a strict development schedule, acceptance criteria, a control mechanisms were put into place.

In January 2005, the IOC was deployed as scheduled; however, a critical report from the inspector general was released in February. At the same time, the report on VCF commissioned to Aerospace Corp began circulating on Capitol Hill. At a hearing on February 3rd, Senator Judd Gregg (R-N.H.) said, "the [VCF] architecture was developed without adequate assessment of alternative and conformance to various architectural standards, and in a way that precluded the incorporation of significant commercial off-the-shelf software. Furthermore, high-level documents, including concept of operations, systems architecture, and system requirements were neither complete nor consistent, and did not map to the user needs. [Finally] the requirements and design documentation were incomplete, imprecise, requirements and design tracings have gaps, and the software cannot be maintained without difficulty. And it is therefore unfit for use." (U.S. Department of Justice, 2005).

A Train Wreck in Slow Motion

The project's lack of progress also drew public criticism from Senator Patrick Leahy (D-Vt.), who said "the FBI's long-anticipated Virtual Case File has been a train wreck in slow motion, at a cost of $170 million to American taxpayers and an unknown cost to public safety" (Hayes, 2005).

The IOC project ended in March, and according to an internal FBI assessment, "Although the IOC application was an aid to task management, its use did not improve the productivity of most users." In fact, most FBI agents found that the IOC increased their workloads because agents had to fill out forms electronically and then route them for superiors for approval. The electronic form was then uploaded to the ACS, which was still in use. However, the form still had to be printed, routed, signed, and filed to comply with the FBI's paper-based records management system (Goldstein, 2005).

The FBI was faced with trying to salvage the debacle project and appease a growing number of critics who believed that the four-year-old project was a waste of taxpayer money (Rosencrance, 2005). Moreover, Robert Mueller confided to reporters that while the VCF project has not been scrapped, the FBI has asked another contractor to look for commercial or government off-the-shelf software packages that could be used instead.

Moreover, Duane Andrews, SAIC's chief operating officer, said "The FBI modernization effort involved a massive technological and cultural change, agency wide. To add to that complexity, in the time that SAIC has been working on the Trilogy project, the FBI has had four different CIOs and 14 different managers. Establishing and setting system requirements in this environment has been incredibly challenging" (Hayes, 2005).

One FBI official remarked that this experience has led to a number of lessons learned in contract management, and this particular contract has led the agency to change its IT contracting practices and develop an IT roadmap. The official also added, "It's definitely not fair to say we haven't gotten anyplace. We haven't gotten the overarching program we wanted, but we're going to take these lessons and move forward with it" (Robb, 2005).

In April 2005, the FBI officially terminated the Virtual Case File project and announced that it would develop a new case management system called Sentinel. This announcement was made by Robert Mueller during his testimony before a subcommittee of the U.S. House Appropriations Committee. Mueller said "I am disappointed that we did not come through with Virtual Case File." However, he added that he sees the decision to cancel the project as an opportunity to use off-the-shelf software to create a more up-to-date system that will allow FBI agents to share information about cases more easily (Rosencrance, 2005).

Robert Mueller stated that the new case management system will be implemented in four phases and should take about 39 months to complete. He was unwilling, however, to estimate how much the new system will cost (Rosencrance, 2005).

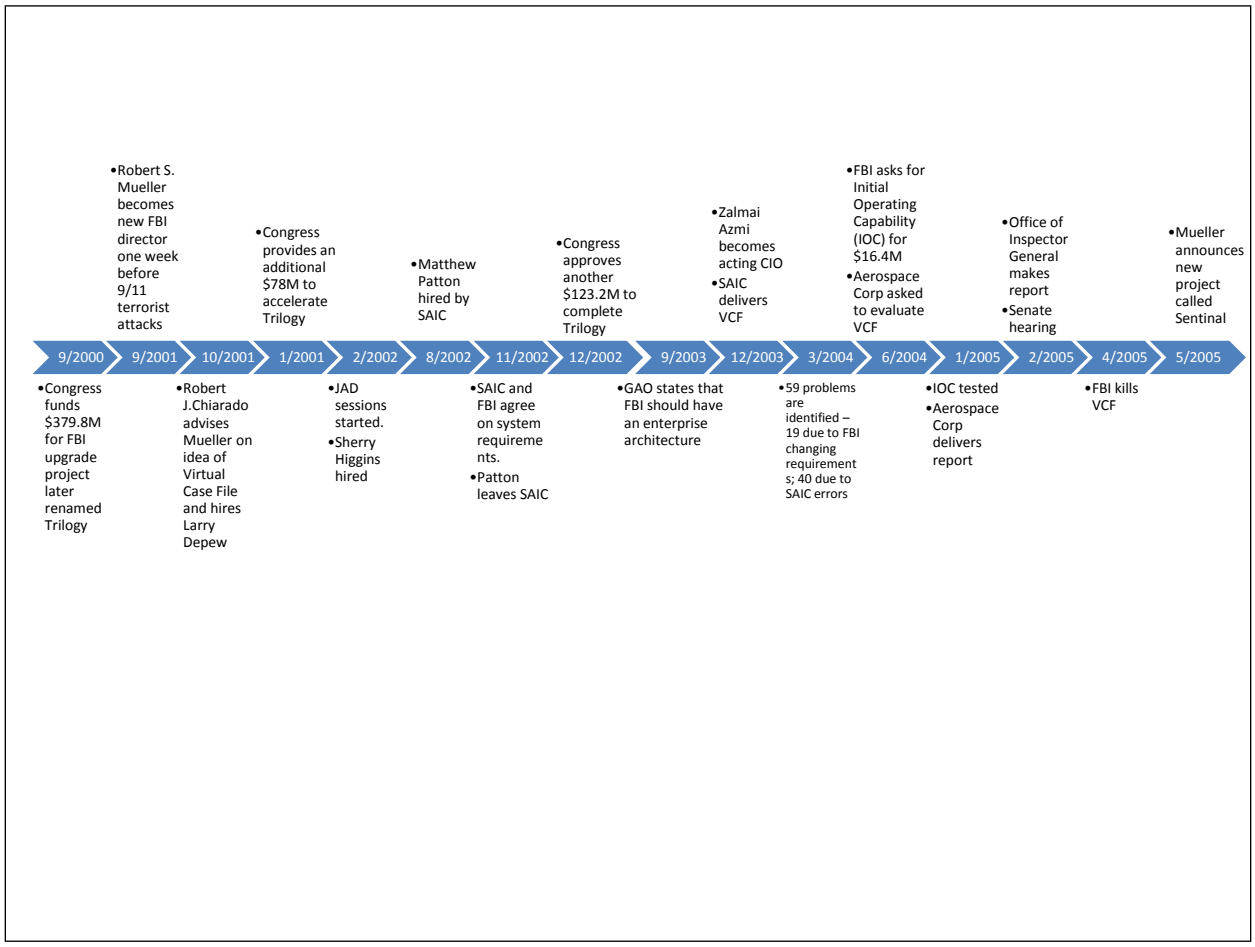

Figure 2: Timeline of Events (Adapted from Goldstein, 2005) .

DISCUSSION

Some FBI agents refer to the Trilogy project as "Tragedy," because it shared characteristics of many failed projects: the best intentions, catastrophic communication, and staggering waste

(Knorr, 2005). To better understand this failure, the US National Academy of Science provided an in-depth study that outlines the reasons for the failure of the Trilogy program and the VCF system (Alfonsi, 2005). The study is called "A Review of the FBI's Trilogy Information Technology Modernization Program," by McGroddy and Lin (2004), and four significant areas were identified: enterprise architecture, system design, program and contract management, and human resources.

According to McGroddy and Lin (2004), the FBI failed "as a matter of its highest priority" in crafting an enterprise architecture to define a strategic view of its goals, mission and needs that could be linked through information technology to its operations and processes. As a result, the FBI could not determine how such investments could be tied to its operational objectives. Moreover, the committee concluded that "the FBI's efforts and results in the area of enterprise architecture are late and limited, and fall far short of what is required."

The second area of concern reported by McGroddy and Lin (2004) centers on System Design, or, more specifically, the FBI's plan for a "flash cutover" from the old ACS to the new VCF. Their opinion was that a limited initial rollout would provide an early warning for potential problems. Moreover, the committee expressed its concern that the rapid development approach and compressed project schedule presumes success at every stage and did not give adequate consideration to testing. This would in effect implement a prototype throughout the bureau where users would most likely be the testers after implementation.

Thirdly, the committee expressed serious concerns regarding the approaches and processes used to develop its IT infrastructure and applications. A major weakness included the lack of "user-vetted prototypes in its applications development processes." Even the most experienced IT professionals cannot anticipate all of the functional requirements and specifications, so internal and contracted developers should make use of extensive prototyping and usability testing with real users. The notion is that iterative development with ample user feedback and involvement increases the likelihood of delivering a system that meets their needs.

Lastly, McGroddy and Lin (2004) identified human resources and external constraints as the fourth area of concern. They point out that the FBI does not have an adequate human resource and skill base needed to deal with the FBI's modernization project. For example, they point out that the FBI had an extreme shortage of experienced project managers, contract managers, and senior IT managers with good communication skills. On the other hand, the FBI hired highly qualified IT professionals "without requiring them to make excessive financial sacrifices, and to borrow personnel from other agencies and even from the private sector." Furthermore, the FBI operates under a number of external constraints that inhibit its flexibility. For example, congressional approval is needed to take any actions or make any changes that exceeded $500,000. The committee pointed out that such constraints are inconsistent with the expectation that the FBI could move quickly to redesign itself and deal effectively with new challenges.

The CHAOS studies (Standish Group, 2005) also report factors for unsuccessful projects, and therefore may provide some insight as to why the VCF project failed. For example, Table 1 summarizes the project factors for not-so-successful projects. This list provides an interesting

thread that can be applied to the VCF project since it appears that the VCF project suffered from many of these same maladies.

As can be seen in Table 1, lack of user input or involvement ranks at or near the top in factors listed under challenged or failed (impaired) projects. Without close support of key users, the team will have a difficult time understanding and defining the requirements of the project. As a result, suspicion and conflicts may arise, and there can easily be an "us versus them" situation between the developers and the users. Without effective communication and a clear direction, changes to the project's requirements always seem to appear, and both the users and developers may set unrealistic expectations. Management then begins to find fewer reasons to support an unpopular project, and more and more resources may be diverted from it.

Rank	Factors for Challenged Projects	Factors for Failed (Impaired) Projects
1	Lack of user input	Incomplete requirements
2	Incomplete requirements	Lack of user input
3	Changing requirements & specifications	Lack of resources
4	Lack of executive support	Unrealistic expectations
5	Technology incompetence	Lack of executive support
6	Lack of resources	Changing requirements & specifications
7	Unrealistic expectations	Lack of planning
8	Unclear objectives	Didn't need it any longer
9	Unrealistic timeframes	Lack of IT management
10	New technology	Technology illiteracy

Table 1: Summary of Factor Rankings for Challenged and Failed (Impaired) Projects. (Standish Group, 1995)

More recently, however, according to a Web-based poll conducted by Computing Technology Industry Association (CompTIA), nearly 28 percent of the more than 1,000 respondents said that poor communication is the number one reason for project failure, followed by insufficient resources (18 percent), and unrealistic schedule deadlines (13.2 percent) (Rosencrance, 2007).

Also illustrated in Table 1 are a number of factors relating to challenged and failed projects that can be attributed directly or indirectly to poor communication. Insufficient resources can be tied closely to poor communication as all projects require resources in terms of people, technology, and facilities. Communication is important in understanding the appropriate number of people that will be needed, what skill sets they will need, the training that may be necessary, and the tools to do the job. Communication is an important component throughout the project in terms of setting project expectations, requirements, as well as schedule and budget constraints. It appears that the VCF project had a number of communication problems throughout its history.

Similar to what occurred during the VCF project, executive sponsors may accept schedule commitments from developers who offer no evidence that they can meet those commitments, while developers may accept schedules that are unrealistic. Not getting the right resources when they are needed may create a risk that the schedule will not be met. Unrealistic schedules may doom the project before it even starts. According to a CompTIA poll, other factors that contribute to project failure include poor project requirements, lack of stake-holder buy-in/support, undefined project success closure criteria, unrealistic budget, insufficient or no risk planning, and lack of control/change process. These warning signs may include strained relationships among the project team members or between the project team and the client or users, excessive overtime, lost confidence, threats of legal action by the customer or client, and low project stakeholder moral. It appears that the VCF project had similar signs of impending failure.

LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

All research studies have limitations and this study is no different. This study provided a single case study of a failed U.S. Government project. It appears that the VCF project had many of the warning signs and characteristics associated with failed projects described in empirical studies over the past fifteen years. However, this is one case study, so future research should include other projects in order to provide a rich qualitative understanding of why and how projects fail. Unfortunately, this may be limited to government projects since most IT project failures by private companies may have limited information or exposure to public view.

However, this may open a door for action research or further empirical research to further our understanding of project failure, or, rather, the ability to improve the likelihood of project success.

REFERENCES

Alfonsi, B. (2005, May). FBI's virtual case file living in limbo. *IEEE Security & Privacy,* 3(2), 7. doi:10.1109/MSP.2005.41.

Al Neimat, T. (2005). Why IT projects fail. Retrieved from www.projectperfect.com.au

Eggen, D., & Witte, G. (2006, August 18). The FBI's upgrade that wasn't. *The Washington Post*.

FBI Congressional Testimony. (2005). Retrieved from www.fbi.gov/congress05/mueller020305.htm

Goldstein, H. (2005, September). Who killed the virtual case file? *IEEE Spectrum*.

Grimes, S. (2005, March). FBI case management system marked for termination. *Intelligent Enterprise*.

Hayes, F. (2005, May 30). FBI on the move. *Computerworld*.

Knorr, E. (2005, March 21). Anatomy of a disaster: How the FBI blew it. *InfoWorld*.

McGroddy, J. C., & Lin, H. S. (2004). A review of the FBI's trilogy information technology modernization program. National Research Council: The National Academies Press.

Merriam, S. B. (1988). *Case study research in education: A qualitative approach*. San Francisco, CA: Jossey-Bass.

Marchewka, J. T. (2009). *Information technology project management: Providing measurable organizational* value (3rd ed.). New York, NY; John Wiley & Sons.

Rosencrance, L. (2005, March 14). FBI scuttles $170M system for managing investigations. *Computerworld*.

Rosencrance, L. (2007, March 9). Survey: Poor communication causes most IT project failures. *Computerworld*.

Robb, D. (2005, May 30). All together now. *Computerworld*.

Standish Group. (1995). Chaos. West Yarmouth, MA; The Standish Group.

Tata Consultancy Services. (2007). Retrieved from http://www.tcs.com/news_events/press_releases/Pages/ITprojectunderperformanceacceptedasthenormbyglobalbusinessmanagementresearchreveals.aspx

U.S. Department of Justice. (2005). The federal bureau of investigation's management of the trilogy information technology modernization project. Office of the Inspector General Audit Division. Audit Report: 05-07.

Verton, D. (2003, April 1). FBI has made Major progress, former IT chief says. *Computerworld*.

Yin, R. K. (1994). *Case study research: Design and methods* (2nd ed.). Thousand Oaks, CA; Sage Publications.

This Page left Intentionally Blank