Volume 7, Issue 1
February, 2014
ISSN: 1946-1836

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

In this issue:

The **Journal of Information Systems Applied Research** (JISAR) 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 currently quarterly. The first date of publication is December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

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 JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org.

2014 AITP Education Special Interest Group (EDSIG) Board of Directors

JOURNAL OF
INFORMATION SYSTEMS APPLIED RESEARCH

The De-Escalation of the DHS HSIN Next Gen Project

Alan F. Rosenhauer
Afr2k@mtmail.mtsu.edu

Melinda Korzaan
Melinda.Korzaan@mtsu.edu

Computer Information Systems
Middle Tennessee State University
Murfreesboro, TN 37132, USA

Abstract

In the eight years since its creation, the US Department of Homeland Security (DHS) had tried to provide a platform for the federal government to share sensitive but unclassified (SBU) information among its varied mission partners. These partners include federal agencies and state and local public safety and law enforcement officials. Its third iteration was under development and was behind schedule, over budget, and was not garnering the support from either management or the user community. The US Office of Management and Budget (OMB) had halted any additional spending on the project. The existing course of action was not acceptable and de-escalation was required. A review of the project led DHS to cancel the project, re-scope the work, and start over. This case study examines the process of de-escalating the project by mapping the de-escalation phases of DHS Homeland Security Information Network (HSIN) Next Gen into an established research framework (Keil & Montealegre, 2000). The study confirms the practical application of Keil and Montealgre's de-escalation framework and provides insights for practitioners from the case's lessons learned.

Keywords: DHS HSIN Next Gen, project management, failed projects, de-escalation.

1. FAILED PROJECTS

Project Failure

Imagine dreaming of a new house, taking the time to draw up blueprints, buy the land, and hire a contractor. You expend time and money digging the foundation, framing the structure, finishing the interior, and landscaping the outside. Then, after all of that work, you decide that you really do not want a new house so you tear down the new house and leave an eye sore of a broken foundation behind for all of the neighbors to see. This may seem like a silly example in the context of building houses but it happens all too frequently when building software applications.

The list of software projects that never reach production is staggering. The US Federal government spent $4 billion for a new IRS computer system and never used it (Charette, 2005). The US Federal Aviation Administration spent $2.6 billion on a new air traffic control (ATC) system and cancelled the project before it went to production (Charette, 2005). The FBI had the Virtual Case File (VCF) system built for a total project cost of $581 million and never used it. The VCF contained over $105 million in unusable code (Goldstein, 2005).

Project failure is not limited to the federal government. After seven years of development, the state of Tennessee cancelled a new health department system. The project had cost nearly $20 million (Gonzalez, 2013). After spending $200 million on a new purchasing system, Ford Motor Company terminated its Everest system (Sherriff, 2004).

Unlike a spectacular failure in the civil or mechanical engineering realm, failures in the computer software discipline often go nearly unnoticed. On July 1, 1940, the Tacoma Narrows Bridge opened near Tacoma, Washington. At that time, the bridge was the third longest suspension bridge in the world. A little over four months later, on November 7, 1940, a 42 mile per hour wind caused the bridge to oscillate and collapse (Billah & Scanlan, 1991). News reporters captured the dramatic collapse on film. For the past 70 years, educators have used the film as a teaching tool and shown it in nearly every high school and college physics class. In 2013 dollars, the bridge would cost approximately the same as the unused FBI VCF code ($106 million). The resulting analysis of the bridge failure showed the root cause of the problem. The solid steel beams did not allow the proper flow of air around or through the structure. The state of Washington devised a solution to the problem and built a new bridge at the same location. The new bridge has been standing and handling vehicular traffic for over 60 years.

As the software industry matures, it must examine the failures and identify the root cause or causes of the failures. A survey of IT projects shows that 18% of the projects failed to deliver the desired outcome or the organization terminated the project before release (PMSolutions, 2011). The same survey showed that 25% of the projects were at risk but the organization was able to recover the project.

Sometimes an organization can recognize the indicators of pending failure. During the construction of the Tacoma Narrows Bridge, the workers noticed that the road surface moved on windy days. The workers affectionately called the bridge "Galloping Gertie" (WS DOT, 2005). Engineers were working on a fix for the "fluttering" of the bridge and on the morning of the collapse were working on obtaining quotes for a solution for the instability. Instead of realizing that the unusual bridge movement was a warning sign for bridge failure, the engineers thought was a minor issue and that they could fix the problem after the bridge was in use. They simply ran out of time.

In the computer world, potential problems are often visible long before the project fails. These warning signs can prompt the project manager to take action before the project comes crashing down around them.

The De-Escalation Process

When a project exhibits warning signs, like a missed deadline or insufficient stakeholder involvement, the project manager must decide between two paths: escalation or de-escalation. Escalation is defined as "continued commitment to a previously chosen course of action in spite of negative feedback" (Keil, Mann, & Rai, 2000). In contrast to escalation, de-escalation is a "reduced commitment to a failing course of action" (Montealegre & Keil, 2000). The goal of de-escalation is to rescue the project and to produce a viable and useful product. The rescue may include a radical re-scoping or a redefinition of the project itself (Montealegre & Keil, 2000). However, sometimes the project manager is unable to salvage the project and must terminate the project. Previous research discusses the process to decide between escalation and de-escalation (Staw, 1976; Keil, 1995; Keil, Mann, & Rai, 2000; Lunenburg, 2010). Studies have also emphasized the importance of organizations being aware of effective de-escalation strategies to prevent future projects from escalating out of control and unnecessarily wasting valuable resources (Pan, Pan, & Flynn, 2004).

Similar to the series of steps during the start of a project, projects often follow a defined series of steps during de-escalation. Research by Keil and Montealegre (2000) proposed a four-phase process for de-escalating a project: 1) problem recognition, 2) reexamination of prior course of action, 3) search for alternate courses of action, and 4) implementation of an exit strategy.

The remainder of this paper presents a case study into the de-escalation of the DHS HSIN Next Gen project. The researchers gathered the information for this case study through interviews with current and former DHS employees, email correspondence from the project, and a review of public records available on the Internet. See Appendix 1 for a list of the interview questions.

The information presented will identify some of the project's escalation warning signs, detail the actual de-escalation process following the four phases of the Keil and Montealegre (2000) model, and provide insights into specific lessons learned from the project.

2. BACKGROUND

The United States federal government created the Department of Homeland Security in response to attacks of September 11, 2001. One of the stated functions of DHS was to provide a mechanism for the federal government to share information with state and local authorities. (Homeland Security Act of 2002) Many of the existing agencies that merged into DHS were already sharing information with state and local officials but these different sharing capabilities led to silos of information. It was this compartmentalization of information that kept law enforcement from identifying the plans of the 9/11 terrorists. DHS needed a platform that would allow the sharing of information across both the levels of government (federal, state, and local) and across the type of government (law enforcement, immigration, intelligence). In order to expedite the deployment process, DHS began looking for an existing system to meet their needs.

The Joint Regional Information Exchange System (JRIES) was an information sharing system that was born out of a specific need to share information between the California Anti-Terrorism Information Center (CATIC), the New York Police Department, and the Defense Intelligence Agency (DIA). DHS decide to adopt the JRIES system as their means to share sensitive but unclassified (SBU) information. At the time, the JRIES board of directors welcomed the addition of DHS to the program. The JRIES system used Microsoft's Groove application to share documents and allow collaborative editing of those documents. It also used the open source Jabber software for instant messaging. While JRIES satisfied the need for document sharing and instant messaging, it did not include any other collaboration tools. In September of 2003, DIA transferred control of JRIES to DHS and in February of 2004, DHS renamed JRIES to HSIN. DHS quickly expanded the JRIES membership to include members from all 50 states. With the increased number of users, the JRIES platform started to suffer performance problems. In order to handle the increased workload and to satisfy additional customer requirements, DHS converted the HSIN site to Microsoft SharePoint 2003 in March of 2005.

Unrelated to its technology decisions, the HSIN program started to experience issues with fulfilling its stated mission goals. In fact, the program had critics inside DHS, in Congress, and in the anticipated user community. In May of 2005, the JRIES board of directors voted to discontinue their relationship with HSIN. They cited concerns over the changes DHS was making without the input from the affected stakeholders. Law enforcement personnel expressed confusion between the seemingly overlapping missions of the FBI's Law Enforcement Online (LEO) and the Regional Information Sharing Systems (RISS) RISSNET services. By January 2006, DHS mandated that all components of DHS were to use HSIN for its information sharing initiatives. About that same time, the DHS Office of the Inspector General (OIG) conducted an audit of HSIN. In its June 2006 report, the OIG reported that DHS did not clearly define HSIN's role, that HSIN's efforts to solicit input from all HSIN user communities were "inadequate", and that it did not clearly define its relationship with other information sharing systems. Also in 2006, 13 US Representatives issued a report identifying 33 unfulfilled promises from DHS. Of the 33, three specifically referred to HSIN. In May of the following year, Congress held a hearing concerning HSIN. At that hearing, Rep. Jane Harman (CA) stated that after three years, instead of having a "robust system", HSIN was "kind of a mess" (US House of Representatives, 2007).

The Next Generation

By the fall of 2007, pressure on DHS to fix the HSIN program caused it to look for alternatives. In October of 2007, DHS decided to upgrade HSIN to a new platform and to include new capabilities. DHS named this new version HSIN Next Generation or HSIN Next Gen. DHS referred to the currently deployed instance of HSIN as HSIN Legacy. The project consisted of four phases or spirals. (US Government Accountability Office (GAO), 2008) In the first phase, HSIN Next Gen will establish an operational platform for 20,000 new users from the critical infrastructure user community. The next phase begins the migration of the existing HSIN Legacy users to the new platform. The third phase completes the migration of users and phase four provides improved content management, better information discovery and delivery, and improved notification capabilities.

Key Target Dates	
May 2008	Project Start
August 2008	Phase 1 Complete
May 2009	Phase 2 Complete
September 2009	Phase 3 Complete
November 2009	Phase 4 Complete

Table 1

See Appendix 2 for the complete timeline.

The Advisory Committee

Shortly after the announcement of HSIN Next Gen, DHS created the HSIN Advisory Committee (HSINAC). The initial HSINAC meeting took place at the end of October 2007 (HSIN Advisory Committee, 2007). At this meeting, a HSIN representative listed two important items. DHS did not have a "preordained path" for HSIN and that the HSINAC would not be briefed on the Next Gen project. Their intention was to keep the deliberations of the HSINAC unbiased. A HSIN representative stated that the HSAINAC should not focus on technical requirements but instead focus on policy and governance issues. The HSINAC recommended that DHS create a governance board consisting of federal, state, local, and tribal partners. The purpose of this board would be to define business processes and workflows. At the conclusion of this initial meeting, the HSINAC recommended that HSIN become the "one-stop shop" for unclassified information sharing. This all-encompassing scope would prove to be problematic for HSIN. At the second HSINAC meeting, the committee recommended that DHS create a Configuration Control Board (CCB) to manage the process of gathering requirements. At the third meeting in July 2008, a committee member stated his concern that the development was proceeding at a rapid pace without the proper management and control procedures (HSIN Advisory Committee, 2008). DHS assured the committee that the proper control measure would be in place 6 months into the project and that full management controls would be in place by July 2009 when the program was scheduled for deployment.

The HSIN Next Gen Project

DHS was experiencing their own growing pains and the Next Gen project was a victim of those difficulties. The creation of DHS was a significant undertaking that included both the establishment of a new department but it also included the reassignment and restructuring of many existing federal government agencies.

At the same time that DHS was proposing the Next Gen project, the GAO was faulting DHS for not having a full set of management controls in place for acquisitions (GAO, 2008). The GAO report specifically faulted DHS for not having a program office and for not identifying staff roles and responsibilities, for not having established a process to gather, analyze, and validate user requirements, and finally for not having a risk management plan in place. DHS staff used their own aggressive schedule as justification for proceeding without the controls in place. Additionally, DHS had not published a departmental System Life Cycle (SLC) framework and it did not complete its product acquisition policies until more than two years after the project went out for bids.

The Next Gen project also included the consolidation of 28 other web portals deployed within DHS. Each web portal had its own unique user community, workflows, and requirements. The HSIN staff at that time consisted of an average of five full-time federal employees. HSIN staff needed to hire an outside consultant/contractor to design, develop, and deploy the system. Throughout the development of Next Gen, the HSIN full-time staff experienced significant turnover with only two full-time staff remaining in the same job for the entire project, one in management and one support staff. The team also had one contract worker converted to a full-time federal employee.

The bid process took just nine months and only two vendors responded. DHS awarded General Dynamics with the contract in May of 2008 with an initial budget of $18M and a potential five-year value of $62M if DHS exercised all the options. The Next Gen project envisioned a brand new platform with state-of-the-art technology. Unfortunately, that vision did not pan out. The contract with General Dynamics did not contain the specificity required in a project of this size. Instead of focusing on specific use cases needed for each user community, the Next Gen requirements included a series of generic capabilities and features and did not include specific information sharing processes and workflows.

3. MAPPING THE DE-ESCALATION PROCESS

Although the HSIN team did not specifically model their de-escalation on the model proposed by the Keil and Montealegre (2000), the steps of their de-escalation mapped well to the model.

Step 1: Recognizing the Problem

The first step in the Keil and Montealegre (2000) de-escalation process is the recognition of a problem. This may take the form of negative feedback about the project or it may include external pressure on the project. The Next Gen project had many entities questioning its chance for success.

Problems Arise with Next Gen

The contractor had barely begun the process of creating HSIN Next Gen when problems started to arise. In July 2008, two senior members of the US House of Representative sent a letter to DHS Secretary Chertoff (Lipowicz, 2008). They asked the secretary to halt all work on HSIN Next Gen until the program's state, local, and tribal users had defined and validated all the requirements. The representatives felt that DHS left the non-federal users out of the requirements gathering process and that DHS had not identified the needs of the non-federal users. In its response, DHS defended its procurement process and stated that the requirements addressed the needs of state, local and tribal user, but ultimately DHS did not change the requirements nor did they solicit additional input from its partners in state, local, and tribal organizations. The representatives were concerned that HSIN Next Gen was repeating some of the mistakes of HSIN Legacy.

Methodology Questioned

In addition to the poor requirements, HSIN staff felt that General Dynamics focused too much on the technology and not enough on the mission. The General Dynamics team started with a variety of off-the-shelf software products and then customized each of them to meet the needs of HSIN. They selected Oracle for identity management, EMC Documentum for their content management system, RSA for two-factor authentication, and Adobe Connect for conferencing and instant messaging. While each of these products is a quality application, the development team struggled to get all of the parts to work together. The development team had to contend with external requirements that were difficult to incorporate into the suite of products. The RSA solution chosen by General Dynamics used one-time-passcode tokens for two-factor authentication. However, Homeland Security Presidential Directive number 12 (HSPD-12) mandated the use of Personal Identity Verification (PIV) cards for all government employees and contractors. The directive required that all agencies issue the new cards by October 2008. DHS did not meet that deadline. In 2010, they had still not met the directive. Since the RSA tokens were not the stated direction for authentication, DHS never issued the cards and thousands of them sat unused in storage.

HSIN hacked

In the middle of the development of the Next Gen version, the Legacy version of HSIN suffered two attacks by hackers, the first in March 2009, and the second in April 2009 (Lipowicz, 2009). The attack forced DHS to shift resources from the new system to bolster security on the old system. It also reinforced the need to replace the Legacy system and to implement two-factor authentication on Next Gen.

The Schedule Slips

The initial project plan called for a HSIN Next Gen deployment in November 2009. The HSIN team did not meet that deadline. Part of the platform was available for use but most of the required components were not available for use. Only one group of users had been migrated to the new platform and most users could not be migrated until the remaining capabilities were available. Interoperability with LEO and RISS was not functioning.

Groupthink

The HSIN team had a significant turnover and many of the General Dynamics team members had a longer tenure on the project. Subsequently, the HSIN team did not feel they had the authority to question publically some of the decisions or even question the overall viability of the Next Gen project. For much of the project the contractors outnumbered the federal staff. DHS delegated or abdicated many important policy and direction decisions to General Dynamics. To complicate matters more, General Dynamics sub-contracted some of the work creating even more layers of bureaucracy.

Work Stops

Others noticed the delays in the Next Gen project. The DHS Inspector General reported that even groups within DHS were not using

HSIN. Many DHS Fusion Centers reported that they stopped using HSIN because of the limited content and the lack of regular updates to the information. When HSIN purged Fusion Center accounts that had not been used in six months, the number of accounts dropped from 7,000 to 1,000. The Office of Management and Budget (OMB) reviewed the HSIN program in early 2010. OMB designated the HSIN program as a high risk and ordered a stop to all development work. OMB then conducted a review to determine if the program would receive any additional federal funding. The review found that HSIN was a viable program but OMB added conditions to any additional funding. The system must improve its interoperability with other systems, expand its user base, and accelerate the consolidation of the other DHS portals. The OMB review also identified a problem with the ownership of the Next Gen project. The report faulted DHS for having the DHS Office of Operations Coordination and Planning (OPS) run both the HSIN program and the Next gen project. DHS OPS was not an IT-based organization. The management of the Next Gen project transitioned to the DHS Office of the Chief Information Officer (OCIO) while the overall project remained under the control of DHS OPS.

Step 2: Reexamining the Present Course of Action

The second step in the de-escalation reexamines the decisions and plans of the current course of actions (Keil & Montealegre, 2000). This step requires management to look at the project objectively and to analyze the available information. The various stakeholders may try to pull the project in different directions. Some stakeholders may want to stay the course, while others will want to change or cancel the project. This step requires the project manager to redefine the project based on the latest information.

Decisions

The new OCIO staff had to make some decisions. The current implementation was failing and they needed to identify an alternate plan of action. They needed to analyze the situation and determine a root cause. Once they identified the root cause, or causes, they needed to decide on an escalation path or a de-escalation path. If the program was failing due to a lack of budget or staff, escalation might be the solution. If the problem was a process problem, cancelling the project may be the best course of action. Ideally, an outside consultant would look at the problem objectively. Based on the OMB funding stoppage, that was not possible. Instead, the OCIO staff created a "tiger" team to look at the problem. In the DHS parlance, a tiger team is an ad hoc group created for a single purpose and would focus using the "eye of the tiger." The team consisted of the newest members of the staff, because management felt that the newer team members would have less emotional attachment to the current solution and would thus be more objective.

The team started by identifying the required capabilities of the program. DHS had given an initial set of requirements to the General Dynamics. However, those requirements did not encompass the complete set of needs from all of the user communities and it did not include the new requirements added during the development. The tiger team analysis identified 61 operational capabilities that the system must support. The team then looked at the capabilities of the existing systems. The original HSIN Legacy system met 84% of the operational capabilities. Another existing portal, HSIN State and Local Intelligence Community of Interest (SLIC) met 35% of the capabilities. The team also found that the new Next Gen application met only 51% of the operational capabilities.

The team also found that if DHS consolidated the 28 different portals spread throughout DHS, DHS would save an additional $50M a year. The tiger team felt that the HSIN program provided a needed resource to their user community and a properly planned and executed upgrade would save the department money in the end.

The team sent their results to the HSINAC. The HSINAC accepted their results and recommendations. The tiger team then forwarded their results to DHS management. During the interviews, HSIN Staff indicated that a DHS independent verification and validation (IV&V) review corroborated the recommendations of the tiger team.

Step 3: Searching for Alternate Courses of Action

The purpose of this step is for the project manager to minimize the damage associated with the current plan and to develop an alternate plan of action (Keil & Montealegre, 2000). The project should rely on independent analysis of both the current plan and the proposed course of action.

A New-New Direction or a New-Old Direction

Identifying that the HSIN program should continue was only half of the story. The tiger team needed to identify a new course of action. When the HSIN team envisioned the Next Gen program, they focused on creating a new platform to share information between the different user communities. The team realized this was an ill-conceived vision. DHS had 28 portals that were already sharing information. The focus of the HSIN program should be on efficiently consolidating the existing portals with the hopes of sharing information among the different groups not just within each of the groups.

DHS initiated the Next Gen project as a new development effort. The tiger team recommended that HSIN not look at a new development project but instead look at a new version of the old HSIN Legacy system. With the Legacy system scoring higher than Next Gen, the tiger team recommended that HSIN just upgrade Legacy to Microsoft SharePoint 2010 and include the enhanced security of Next Gen. They felt this was the best course of action.

Step 4: Implementing an Exit Strategy

The final step in the de-escalation is the implementation of an exit strategy (Keil & Montealegre, 2000). The project manager must inform the stakeholders of the change in the project plan and then execute the closing of the old project.

Cancelling the Project

The HSIN staff was relieved that the Next Gen project was closing. When the GAO halted their funding, most of the staff focused their energy on the Legacy platform. They also took the opportunity to create a formal requirements document for the HSIN platform.

Unfortunately, DHS could not just turn off the Next Gen platform. The HSIN team had already moved a group of users from FEMA to Next Gen. In addition, HSIN staff had not tested the software for enabling the interoperability with LEO and RISS. This software was part of the enhanced security from Next Gen they wanted to implement in Legacy. However, HSIN could not afford to keep both Legacy and Next Gen running while they built a new version. The team came up with a hybrid plan. The first part of the plan included the migration of the FEMA users to the Legacy platform. The second part consisted of using Next Gen to test the interoperability software with LEO and RISS.

Next Gen Shut Down

DHS officially shut down the Next Gen platform in July 2011. The HSIN team re-scoped the project and work on the next version, HSIN-R3, started in October 2011. HSIN-R3 would not be a new development but instead be a technology refresh where the project team upgraded HSIN Legacy to Microsoft SharePoint 2010, incorporated the improved security features from Next Gen, and included the consolidation of the first ten of the 28 portals.

4. LESSONS LEARNED

Feedback from the interviews provided insight into the lessons learned from the project. The Next Gen project suffered problems from the outset. DHS had a flawed approach to the original HSIN program. DHS took an existing application, JRIES, which was serving a specific community, took complete control of the system, and then alienated the users. In retrospect, JRIES was another portal that they should have consolidated onto a common platform. The users faulted HSIN more with the content of the site than with the technology but the Next Gen project focused on the technology not on the content.

In their effort to provide an all-encompassing SBU portal, DHS focused too much on the technology and not enough on the mission. The contract with General Dynamics was rushed and DHS did not fully vet the requirements with the diverse user communities. HSIN staff felt that the technology was the driver, not the mission. HSIN tried to be the only SBU portal for all of government. Later, they realized that LEO and RISS had a different mission and a different user base. HSIN spent too much effort on those other missions instead of focusing on their users.

The transfer of the Next Gen project from DHS OPS to the OCIO was a necessary action. The OPS office did not have the technical expertise to oversee a development project of that magnitude. The OCIO staff had a departmental-wide purview and ensured that the HSIN program technology aligned with the broader

DHS goals. In addition to the HSINAC that provided input from external sources, DHS created an Executive Steering Committee that set the overall direction of the program. This guidance once again ensured that the program met departmental-wide goals and objectives.

The final lesson learned dealt with user involvement. Most of the targeted user committees felt little or no ownership in the program. DHS usually determined the schedules, requirements, and designs without sufficient input from the users. The Fusion Centers reported that while DHS spent time and effort on the technology, they failed to use the system because of the untimeliness of the data. (DHS OIG, 2010) DHS was working on a technical project when the users needed a content project.

5. CONCLUSIONS

According to Kappelman, McKeeman, & Zhang, (2006), the warning signs for a failing project fall into two categories: people oriented and process oriented. While some of the failings in the Next Gen project were people related, most notably lack of stakeholder involvement at the outset of the project, the majority of the failings were process related.

12 Early Warning Signs

People Oriented

- Lack of top management support
- Weak project manager
- No stakeholder involvement / participation
- Weak commitment of project team
- Team members lack requisite skills / knowledge
- Subject matter experts are overscheduled

Process Oriented

- Lack of documented requires / success criteria
- No change control process / management
- Ineffective schedule planning / management
- Communications breakdown between among stakeholders
- Resource assigned to a higher priority project
- No business case for the projects

(Kappleman, McKeeman, & Zhang, 2006)

Table 2

The project did not have sufficient requirement's definition, DHS did not have well-established processes, the schedules were not realistic, the communications between the end users and the project team were insufficient, and the business case for a complete rewrite was not justified.

In his book, Bennatan (2006) recommends that organizations implement an Early Warning System (EWS) to draw attention to potential problems before the problems become unmanageable. Although there were many warning signs, the HSIN team did not have Early Warning System. With an EWS the team might have been able to rescue the project instead of being forced to cancel the project.

6. CONTRIBUTIONS TO RESEARCH

This case study demonstrates that the de-escalation model of Keil and Montealegre (2000) is still a helpful tool in managing a failing project. This contribution confirms the framework continues to be representative of how de-escalation unfolds in practice.

One use of the case study methodology is to help connect academic research to industry practice and this study provides a case example that confirms the application of the de-escalation framework as a useful guide in studying real world projects as they progress through a de-escalation process. Therefore, academic de-escalation theory continues to generalize to modern information systems' projects, and the continued sustainability of the usefulness of project de-escalation academic theory for practitioner application is confirmed.

Future Research

This study also demonstrates that basic project management practices, like requirements gathering and stakeholder involvement, are lacking. Additional research is called for to identify the reasons behind the lack of proper project management.

The lack of effective project management practices reveals a gap that exists between academic project management / project risk management knowledge and industry practice. The top risk factors that led to the escalation problem with the Next Gen project (such as lack of stakeholder involvement and misunderstood requirements) are the same key risks that have consistently been identified in literature (Schmidt, Lyytinen, Keil, & Cule, 2001; Kappelman, McKeeman, & Zhang, 2006). This is especially salient for stakeholder / user involvement, which has been identified as a key factor in information systems application implementation since the 1960s (Barki & Hartwick, 1994). The question that surfaces is what has industry learned from academic literature in project risk management and why do the same key risk factors continue to be problematic? What can be done to address and prevent these risks before they result in project escalation or project failure?

There is a substantial lack of evidence that academic risk management knowledge is being applied to project management in practice (Taylor, Arman, & Woelfer, 2012). Therefore, a need is identified for future research studies to be conducted collaboratively with both academic researchers and practitioners with a goal to not only identify key risks but also formulate appropriate action plans to be taken early to prevent risk factors from escalating and cause troubled projects later in the project life cycle.

7. REFERENCES

Barki, H., & Hartwick, J. (1994). Measuring user participation, user involvement, and user attitude. *MIS Quarterly*, 18(1), 59-82.

Benbasat, I., Goldstein, D., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, 11(3), 367-386.

Bennatan, E. M. (2006). *Catastrophe disentanglement: getting software projects back on track.* Boston, MA: Pearson Education

Billah, K. Y., & Scanlan, R. H. (1991). Resonance, Tacoma Narrows bridge failure, and undergraduate physics textbooks. *American Journal of Physics*, 59(2), 118. doi: 10.1119/1.16590

Charette, R.N. (2005). Why software fails [software failure]. *Spectrum, IEEE* , 42(9), 42-49. doi: 10.1109/MSPEC.2005.1502528

Department of Homeland Security (DHS) Office of Inspector General (OIG). (2010). Information Sharing With Fusion Centers Has Improved, but Information System Challenges Remain, OIG-11-04.

Eisenhardt, K., & Graebner, M. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, 50(1), 25-32.

Goldstein, H., (2005). Who killed the virtual case file? Retrieved April 29, 2013 from http://spectrum.ieee.org/computing/software/who-killed-the-virtual-case-file/

Gonzalez, T. (2013) State pulls plug on multi-million dollar computer system. *The Tennessean*. Retrieved April 29, 2013 from http://www.tennessean.com/article/20130426/NEWS0201/304260131/

Homeland Security Act of 2002, Pub. L. No. 107–296 § 102. (2002).

HSIN Advisory Committee. (2007). October 31, 2007 to November 1, 2007 meeting minutes. Retrieved March 29, 2013 from http://www.dhs.gov/xlibrary/assets/hsinac_inauguralmtg_2007-1030-1101.pdf.

HSIN Advisory Committee. (2008). July 31, 2008 to August 2, 2008 meeting minutes. Retrieved March 29, 2013 from http://www.dhs.gov/xlibrary/assets/hsinac_mtg_2008-0731-0801.pdf.

Kappelman, L. A., McKeeman, R., & Zhang, L. (2006). Early warning sign of IT project failure: the dominant dozen. *Information Systems Management,* 23(4), 31-36.

Keil, M. (1995). Pulling the plug: Software project management and the problem of project escalation. *MIS Quarterly,* 19(4), 421-447.

Keil, M., Mann, J., & Rai, A. (2000). Why software projects escalate: an empirical analysis and test of four theoretical models. *MIS Quarterly*, 24(4), 631-664.

Keil, M., & Montealegre, R. (2000). Cutting your losses: Extricating your organization when a big project goes awry. *Sloan Management Review*, 41(3), 55-68.

Lipowicz, A. (2009). Information-sharing platform hacked. Retrieved January 21, 2013, from http://fcw.com/Articles/2009/05/13/Web-DHS-HSIN-intrusion-hack.aspx

Lunenburg, F. C., (2010). Escalation of Commitment: Patterns of Retrospective

Rationality. *International Journal of Management, Business, and Administration*, 13, 1-5.

Montealegre, R., & Keil, M. (2000). De-escalating information technology projects: lessons from the Denver International Airport. *MIS Quarterly*, 417-447.

Pan, G., Pan, S., & Flynn, D. (2004). De-escalation of commitment to information systems projects: A process perspective. *Journal of Strategic Information Systems*, 13(3), 247-270.

PMSolutions. (2011). Strategies for Project Recovery. Retrieved April 28, 2013 from http://www.pmsolutions.com/collateral/research/Strategies%20for%20Project%20Recovery%202011.pdf.

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international Delphi study. *Journal of Management Information Systems*, 17(4), 5-36.

Sherriff, L. (2004) Ford dumps $200m Oracle system. Retrieved April 29, 2013 from http://www.theregister.co.uk/2004/08/18/ford_ditches_oracle/.

Simon, A., Sohal, A., & Brown, A. (1996). Generative and case study research in quality management. Part I: Theoretical considerations. *International Journal of Quality & Reliability Management*, 13(1), 32-42.

Staw, B. M., (1976). Knee-Deep in the Big Muddy: A Study of Escalating Commitment to a Chosen Course of Action. *Organizational Behavior and Human Performance*, 16, 27-44.

Taylor, H., Artman, E., & Woelfer, J. (2012), Information technology project risk management: Bridging the gap between research and practice. *Journal of Information Technology*, 27(1), 17-34.

US Government Accountability Office (GAO). (2008). Management Improvements Needed on the Department of Homeland Security's Next Generation Information Sharing System (GAO-09-40). Washington, DC: US Government Printing Office.

US House of Representatives. (2007). Hearing before the subcommittee on intelligence, information sharing, and terrorism risk assessment of the committee on homeland security. (110-34). Washington, DC: US Government Printing Office.

Vissak, T. (2010). Recommendations for using the case study method in international business research. *The Qualitative Report*, 15(2), 370-388.

WS DOT (2005). Tacoma Narrows Bridge. Retrieved April 29, 2013 from http://www.wsdot.wa.gov/TNBhistory/.

Editor's Note:

This paper was selected for inclusion in the journal as the CONISAR 2013 Best Paper The acceptance rate is typically 2% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2013.

Appendices and Annexures

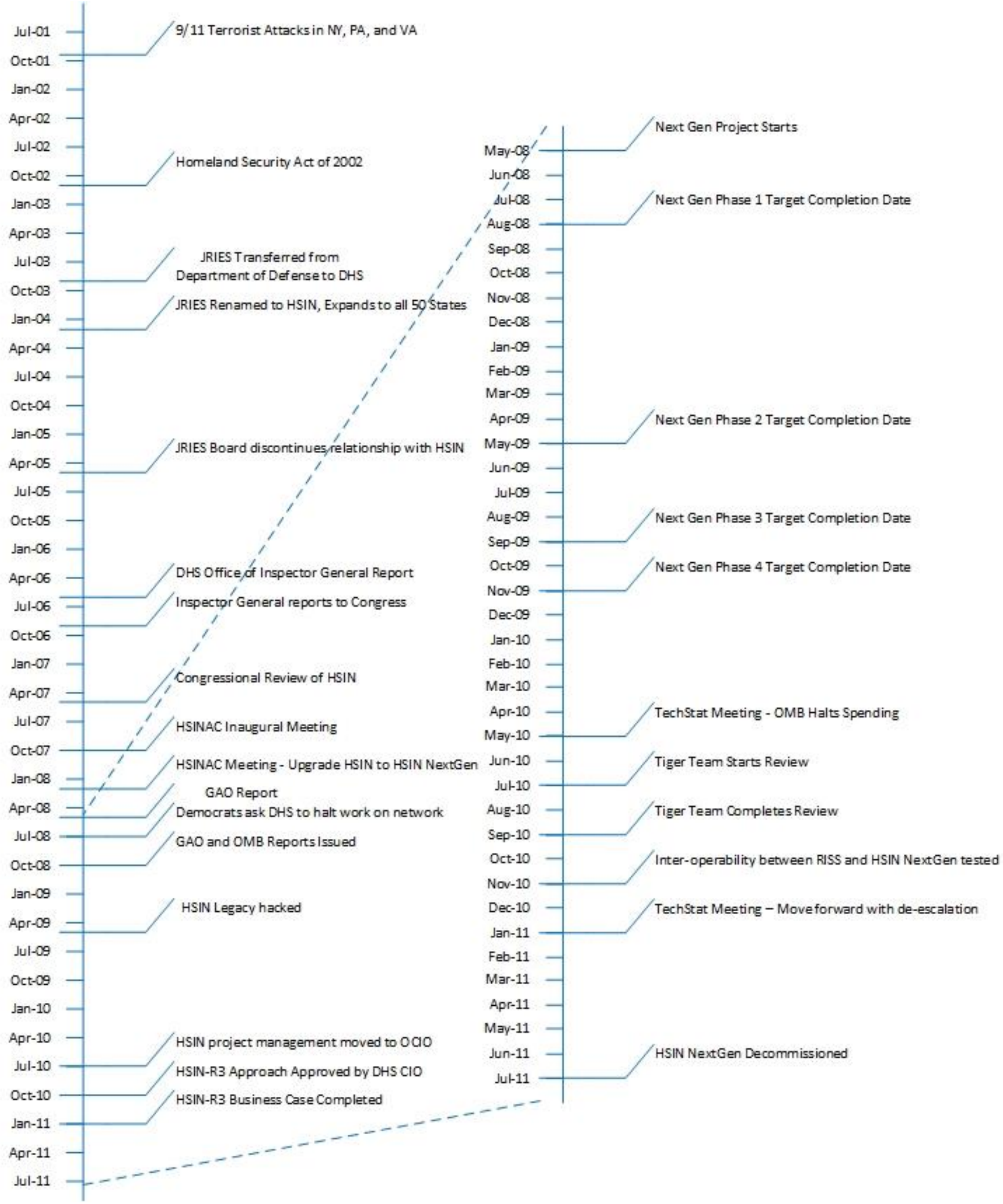
Appendix 1

INTERVIEW QUESTIONS

1. What was your involvement in the DHS HSIN Next Gen project?
2. Describe the process for assessing the project's status.
3. What indicators did you find that showed the project was having difficulties?
4. Describe the steps of de-escalating the project.
5. What was the original expectation of the de-escalation: cancellation, re-directing and re-starting the project, or was any option acceptable? Was the original expectation what actually happened because of de-escalation?
6. How did you inform the team members of the process?
7. What was the team's reaction to de-escalation?
8. What changes did you implement in the re-start of the project?
9. What changes did you make to the overall development process because of the lessons learned in de-escalation?
10. What were the key lessons learned or take-aways from this entire process?

Appendix 2

TIMELINE OF EVENTS


Jul-01
Oct-01
Jan-02
Apr-02
Jul-02
Oct-02
Jan-03
Apr-03
Jul-03
Oct-03
Jan-04
Apr-04
Jul-04
Oct-04
Jan-05
Apr-05
Jul-05
Oct-05
Jan-06
Apr-06
Jul-06
Oct-06
Jan-07
Apr-07
Jul-07
Oct-07
Jan-08
Apr-08
Jul-08
Oct-08
Jan-09
Apr-09
Jul-09
Oct-09
Jan-10
Apr-10
Jul-10
Oct-10
Jan-11
Apr-11
Jul-11
9/11 Terrorist Attacks in NY, PA, and VA
Homeland Security Act of 2002
JRIES Transferred from Department of Defense to DHS
JRIES Renamed to HSIN, Expands to all 50 States
JRIES Board discontinues relationship with HSIN
DHS Office of Inspector General Report
Inspector General reports to Congress
Congressional Review of HSIN
HSINAC Inaugural Meeting
HSINAC Meeting - Upgrade HSIN to HSIN NextGen
GAO Report
Democrats ask DHS to halt work on network
GAO and OMB Reports Issued
HSIN Legacy hacked
HSIN project management moved to OCIO
HSIN-R3 Approach Approved by DHS CIO
HSIN-R3 Business Case Completed
May-08
Jun-08
Jul-08
Aug-08
Sep-08
Oct-08
Nov-08
Dec-08
Jan-09
Feb-09
Mar-09
Apr-09
May-09
Jun-09
Jul-09
Aug-09
Sep-09
Oct-09
Nov-09
Dec-09
Jan-10
Feb-10
Mar-10
Apr-10
May-10
Jun-10
Jul-10
Aug-10
Sep-10
Oct-10
Nov-10
Dec-10
Jan-11
Feb-11
Mar-11
Apr-11
May-11
Jun-11
Jul-11
Next Gen Project Starts
Next Gen Phase 1 Target Completion Date
Next Gen Phase 2 Target Completion Date
Next Gen Phase 3 Target Completion Date
Next Gen Phase 4 Target Completion Date
TechStat Meeting - OMB Halts Spending
Tiger Team Starts Review
Tiger Team Completes Review
Inter-operability between RISS and HSIN NextGen tested
TechStat Meeting – Move forward with de-escalation
HSIN NextGen Decommissioned