

Why Projects Fail – A viewpoint.
Dan Morrill
April 2006

One of the more interesting issues around project failure though is that DRM projects not only rely on inside resources to be success, but outside resources as well. Customers, independent security researchers and ordinary hackers all have a vested interest in the DRM technology chosen by a company. However, given the idea that projects fail, with regularity in that process, the other question is why do information security projects fail, or why do DRM projects fail is a topic of discussion for this blog. In the longer run, regardless of what the project being undertaken is, the regularity in which projects fail has been the subject of research for years. There is a lot of good information about both project failure and project success. The commonalities between project failure research is interesting that between the major reports like the Bull report and the Chaos report, the commonalities are striking year to year.

The Bull report from 1998 indicated that the major cause of project failure were missed deadlines in 75% of cases, exceeded budget in 55% of cases, poor communications in 40% of cases and finally, inability to meet project requirements in 37% of cases. While the major commonalities in project success were meeting milestones in 51% of cases, maintaining quality levels in 32% of cases and meeting budget in 31% of cases. The Bull report builds the argument that the ability to maintain a successful project fall into the category of maintaining deadlines, maintaining budget, maintaining clear communications along the project information chain, and meet the project requirements that were started out with. Threat modeling the project will give a clear indication of where the process is likely to fail, and a strong Project Manager should be aware of these failure points, and develop strategies to ensure that the project is completed in time and meeting all the criteria for success. Project managers should develop contingency plans for the loss of key personnel like management supporters, key technologists, and even the loss of the key Project Manager.

The Chaos report of 1994 was also in line with the Bull report in that projects failed because of lack of user involvement, incomplete requirements, lack of resources, unrealistic expectations, lack of executive support, and a host of other issues focused around management skills, and technology that grew old and obsolete while the project was waiting to be completed. An interesting part of the Chaos report was that executive managers believed that there were more failures today than there were 10 years ago. Given then that, management has a perception of failure, it will be important to approach all projects with the ability to factually reassure management that the project is a timely project. Moreover, that the technology that is mature enough to do the required functions, and that there are contingency plans in the works so that IT and personnel resources are not going to be misused on a project that is doomed from the start.

In any project, including an intellectual property protection project, it is important that anyone starting any project have the ability to complete the project, and understand the technology that is being put in place. Many projects involve new technology that the

company does not have a basis in or the knowledge depth on staff to carry the project through. This in its own right can add to the probability of failure of a project, and is a risk point that should be identified by the project manager early on. Hiring for projects, to bring in much needed information and skills is important in helping the project succeed in the longer run if there is no depth to the IT Staff. Alternatively, if the IT staff is generally unavailable to see the project through to completion, bringing on contractor support may be essential to having the project succeed. As well, if there is a large amount of socialization that needs to happen to find out if the project is really what the end users want, or need. If there is a project for the sake of the project, but no one really wants it, or no one will really use it, there are better ways for the company to spend money. Managers should be evaluating why the project is being undertaken, and that the end-point of the project is to save money, time, or resources. In some cases, like Sarbanes Oxley, HIPAA, GLB, or HR1386, some of the project requirements are in response to a legal dictate or requirement.

Legally mandated projects can be easily socialized as justified within the company, as most employees understand the need to comply with legal dictates. In these kinds of instances, project failure is still a possibility, but executive support, and other support along the company culture is easier to socialize, and easier to devote resources to, as fines and penalties are usually quite stiff in relationship to the end costs of the project. As well, companies that are showing good faith efforts in completing the project can usually get extensions in the regulatory space so that there is time to complete the project and avoid external punishment. Non legally mandated projects have a harder time being socialized within the organization because their need, usefulness, applicability, and ability to support the project will have to be more clearly defined rather than pointing to an external authority and justifying the project in that manner.

The technology that can be used for Intellectual property protection at this time is immature, and while some protection software exists, there is no one product that does everything that a company would need or want. Rather the technology is going to be installed piecemeal which adds to the complexity of the project, and increases its chances of failure. If a company has the technological staff, and ability to manage various software packages that may not work harmoniously, then an Intellectual Property protection project is a good undertaking. If the company does not have the ability to manage this kind of variations in technology, nor do they have a good understanding of forensic searching of various peer to peer networks, then the company should pay for staff to be trained, or hire the appropriate staff to build and do knowledge transfer back to the full time employees.

Project failure is directly tied to the relative immaturity of the products chosen, inability to lead, the lack of executive support, internal adoption of the technology, and the inability to manage or maintain goals, budget, and deadlines. If the project requires a heavy socialization factor in the organization, it is also important to maintain the support and conviction of the employees that this is going to help them in the longer run. Socialization of the project, with clearly stated rewards and risks will assist the company and the employees in doing their daily functions. Alternatively, that this is a strategic

initiative in that the technology has clearly stated rewards, and those statements should come from the executive sponsors and lead project manager as a monthly or weekly project update. Clear disclosure of the project, project status, and rewards will help adoption and support for the project from the company's general population. DRM projects also rely on the external users, security researchers and hacker's adoption or ability to defeat the technology and adapt to it. This additional set of components in a DRM project add to the complexity, and can add to failure of the project, loss of corporate reputations, and like Sony, lead to the loss of money as well.

Projects should not be undertaken because it is the latest technology without a definite need for the new technology. Nor should projects be undertaken to support a political end game that in the longer run does not serve the overall needs of the company from both the strategic and tactical level. Employees will usually see through projects that are politically motivated and not put their full support behind the project, nor will adoption of the technology or project be as successful as it would be under other circumstances. The end user will not see some projects like systems upgrades on the backend support network. Others like upgrading all PC's on the network will be seen by the end user and will usually be adopted or accepted without many problems. The issue will be with the IT team that is working to roll this out, while upgrading the backend infrastructure for the new operating system.

In one instance a key project that was legally mandated, was dubbed "the project that would not die" and while eventually successful, was years over due, and over budget. The project was not socialized correctly, the technologists involved did not understand the product, and the reliance upon external contractors did not include technology and knowledge transfer in the longer run. The company is now tied into a contract arrangement that may or may not make sense in the longer run. As well, all the key personnel that helped install and develop the project have left the company.

Undertaking a DRM project is no different from any other project that a company will take on. There have to be realistic expectations from the start of the project, and there have to be clearly defined boundaries around that process. What is the company trying to protect, does it have a reasonable cost structure, does it have ramifications outside of the company, how does the DRM system escrow or adopt to changes in technology, will there be non DRM'd versions that will be shared with archival, library, or trusted trading partners. Do the technologists who will be implementing the DRM process across the company understand how the technology works, does everyone understand its limitations and has anyone in the company figured out a way to break the process, or use the process for other than intended uses? What other gotcha's can be garnered from the software manufacturer, and are there cases where the technology was used successfully with a minimum of problems for the end users? Is the technology being reviewed mature enough to answer all the requirements from the company, or are there holes in the process that need to be threat modeled?

When approaching a DRM project or indeed any project, knowing what needs to be accomplished, finding the right software, then having the right people in place to

accomplish the work along with executive sponsorship is the key to success with any project. Knowing that DRM software for both company and customer use carries risks, like the Sony Root Kit/DRM system from First4Internet in November 2005 that ended up costing Sony corporate reputation and millions of dollars. Both hackers and legitimate security researchers are reviewing and in many cases disassembling the DRM technology. Nor is DRM technology bug free, as shown by the ability to defeat early DRM technology by holding down the CTRL key while installing customer oriented DRM as discovered by DVD John. While these are both examples of what can go very wrong with a DRM project, there are DRM technologies that exist for product authentication as used in Video Games, or installation keys that use a unique alphanumeric hashing. These technologies are well understood and carry little if any negative responses from end users, and they are usually transparent to end users.

The choice of technology matters, as well as the current adoption of the DRM technology worldwide. While First4Internet was using an adopted technology in the form of a root kit, the negative connotations of the technology, and the idea that it was discovered by legitimate security researchers much to their surprise, the negative connotations and eventual monetary and corporate reputation loss did not in the longer run justify the use of that particular DRM schema. First4Internet is not the only DRM provider feeling that legal resources have turned against them, Suncomm, FairPlay, and others have also faced scrutiny world wide, and in some cases been forced to pay fines, or otherwise watch their corporate reputations suffer harm.

From a project management viewpoint, if the population of consumers what will buy the product reject the DRM mechanisms chosen. As well, having multiple competing DRM schema's on a consumer's computer should also be evaluated as part of the project goals, that two different DRM schemas would not interact negatively on a consumer's computer. Project success and failure have to take into account the eventual end consumer of the product that is bring DRM'd. If the consumer population rejects the product because of the DRM technology chosen, that should be considered a project failure as the product will not be purchased, or recall of the product that will incur major costs to compensate aggrieved users, governments, and other legislative and industry watch dog groups.

While the Bull and Chaos report focus on internal processes that define project success. The choices that a company makes when determining which technology will or will not be used must also meet industry standards and end consumer needs. External processes that influence the choice of technology within the organization are just as important as ensuring project success from the internal corporate decision tree. Project success is both internally and externally driven, with multiple components that need to be justified and satisfied. Companies that want their projects to succeed need to model the project, and ensure that all the elements for success are understood amongst management and the project manager. While technologists and end users within the company need to understand the way that the project will benefit the entire company so that they understand and can support the project. If the product or service extends outside the

company, then end users should also be part of the process and they need to understand the reason for the technology and how well that technology will be supported by them.

The project that is undertaken has commonalities and unique processes that converge to make any DRM based project dependent upon executive management, project managers, inside technologists, inside users, external users and external technologists. The added complexity of adding external users and technologists to the project cannot be fully accounted for, but neglecting them in the project management success/failure modeling will ensure that any DRM choice that deviates from acceptable standards will be negatively received with high cost to the company. DRM technologies that alter or otherwise have the potential to negatively affect the operation of consumer electronics should be avoided. While inbuilt DRM protection mechanisms that do not negatively impact or influence consumer products should be carefully evaluated for effectiveness and ability to stand up to hackers. Those DRM products that will be used exclusively internal to the company should be evaluated for the ability to recover data in a non-DRM'd state depending on the needs of the company. The success of the project depends upon the technology being carefully reviewed by knowledgeable staff or contractors with all the ramifications of the technology and its use carefully evaluated. Contractor or other support staff should also be training company FTE personnel in how the technology works, what it can be used for, and its impacts along with installing or otherwise enabling the technology for the company.

Project success then is dependent upon clear communications, known use, known support for the technology, remaining on budget and on time, and in the case of DRM technologies, the ability for outside entities like end users, hackers and security researchers to accept the technology without negative ramifications to the company either monetary or reputationally. DRM projects are complicated, but the success of a DRM project is dependent upon the traditional standards of project success, with the additional investiture of outside parties and consumers. Failure to integrate those factors into the project will lead to negative responses, and could expose the company to additional liability as evidenced by Sony, First4Internet, Suncomm and others.

References:

http://www.standishgroup.com/sample_research/chaos_1994_2.php

http://www.it-cortex.com/Stat_Failure_Cause.htm

<http://www.drmwatch.com/drmtech/article.php/3573381>

<http://www.ittoolbox.com>