Volume 6 (2006)

Interface: The Journal of Education, Community and Values

8-1-2006

Adversarial Conditions (or Not All Conflict is Necessarily Bad)

Glee Cady

Adversarial Conditions (or Not All Conflict is Necessarily Bad)

Adversarial Conditions (or Not All Conflict is Necessarily Bad)

Posted on **September 1, 2006** by **Editor**

By Glee Harrah Cady <gleecady@gmail.com>

- **Spy vs. Spy**
- Finance vs. Engineering
- Sales vs. Product Management
- Army vs. Navy (at least in **sports**)

Classic conflicts

Most of us have had the idea that ***conflict is bad*** drilled into us from our earliest days. "Avoid fights." "Be nice." "Don't hit your brother." "Please share." "No, you can't run away from home because your big sister is picking on you." Some of us as parents have even said these things ourselves. Or screamed them, depending on how hot and tired and frustrated we were with the children at the time. We are supposed to be good, share our toys, and not hit our playmates/siblings. That kind of conflict, or the highly escalated kind with real lethal weapons is something I still dislike.

There are more kinds of conflict, though. One healthy kind helps us discover new ideas — it's called "discussion." People with differing points of view espouse them, we all evaluate them, good things happen when we decide what to do. I think we all struggle to do this well, even in small, comfortable groups, because basically we'd just like our own ideas to prevail. It's hard to learn that not everyone is "us," but when we do, and can absorb someone else's viewpoint, it can open doors to new opportunity…

Another, more fun kind of conflict, entices us into a story (book, film, play) and keeps us drawn in until the conflict is resolved satisfactorily. Here is author Jenny Crusie on conflict **From the Crusie-Mayer blog site:**

'*You start with your protagonist in trouble and try to get her into conflict on the first page. Trouble*

is not the same as conflict. Trouble is she can't pay the electric bill and her dog is sick. Conflict is a struggle; somebody stole her electric bill payment and poisoned her dog and now she's trying to stop him.'

Now what is Glee babbling about, you ask, citing a novelist in a column about privacy and information security?

Well, the idea that I am espousing is "it's a good thing to have conflict with an objective person who can help your projects by reviewing them." Every good writer is backed by a good editor. Other kinds of activities could use objective review, too.

"Hi, I'm from Risk Management and I am here to help you."

Information Security and Technology Risk Management can be really fascinating, not to mention challenging. A risk manager tries to balance regulations from differing levels of government and standards agencies, corporate polices and rules, and good business practice. Then he or she advises the enterprise about the level of risk acceptable in a project. Or gives advice about the level of risk that will result from *not* doing the project — for example, what might the risk be if we decide to ignore a federal law?

Risk is the possibility that there will be an adverse effect from a particular action.

In risk management, the idea is to determine for each activity, function, process, or project:

1. What are the possible things that could go wrong, (hoping that you will elude Murphy's Law)
2. What is the likelihood that the wrong things will occur, and what can be done to prevent or mitigate the possible adverse action.

And there you have it: risk management — assessment of the risks followed by the assessment and implementation of mitigating controls. It sounds pretty simple when stated this way. The real trick is to recognize which are higher risk activities and develop controls that mitigate those risks, and to effectively advocate that those risks should be addressed by your project team and upper management.

Almost everything we do has risk, getting out of bed, turning left while driving a car, drinking a liquid (we could spill it, it could carry germs, it might be too alcoholic), etc. And the things we do to "be careful" are the mitigating controls.

Standard Technology Risk Categories

In the financial services world, there are categories of risk that we are required to recognize and manage well – or we will suffer the wrath of an "audit finding." In general (since differing schemas

have differing risk categories) the risks fall into *Operational Risks, Credit Risk, Liquidity Risk*, etc. Within Operational Risk, there are categories of risks are those that are most likely to be affected and effected by technology systems:

Transaction risk:

Problems with delivering the service or product. You can think of it as doing the right thing but doing it badly. Some ways to do that are by choosing the wrong platform, the wrong partners, not building in adequate security measures, not planning well for contingencies, etc.

Strategic risk:

Problems with not matching your effort to the goals of the enterprise. Perhaps you built a beautiful product but it was at the wrong time or you built it badly, or by the time you got it built, there was no longer a need for it.

Reputation risk:

The risk you bear should your good name be besmirched, usually by not mitigating some other risk appropriately.

Compliance risk:

The risk you bear by not following the rules and regulations.

In a regulated enterprise, we use the examination guides of the regulators, polices, standards from trade associations, national and/or international bodies (i.e.**ISO 17799**), advice from our internal and external auditors (**ISACA** and **IIA**) — and a big dose of common sense — to build a list of risks that a specific project may face. Here's **a guide** from the US Office of the Controller of the Currency, the regulatory body for national banks. These standards help us identify possible risks.

Once the relevant risks are identified, then it's time to look at their material financial impact and their likelihood. Most of us use some version of a 3 x 3 table to determine the risk level.

Materiality / probability	High	Medium	>Low
High	High/High	Medium/High	Low/High
Medium	High/Medium	Medium/Medium	Low/Medium
Low	High/Low	Medium/Low	Low/Low

Things that are likely to be expensive and very likely to happen or to happen frequently are given a high/high rating. Conversely, things that wouldn't cost much to repair and would not happen often are given a low/low rating. Usually risk that are determined to be HIGH would have ratings of high/high; high/medium; high/low; and medium/high.

Mitigating Risk

Following your assessment, you plan what can be done to lessen the risk – there is really no way to eliminate risk completely. You can only reduce it. You reduce risk my adding controls. The controls can be:

Detective controls – some sort of audit or post-action quality check to confirm that the control is there,

preventative controls – some edit in an online system or pre-action quality check, that prevents bad data from entering the system, or

administrative controls – some rule that you institute. The rule may or may not itself have preventative or detective controls.

Residual risk – the risk that the business decides is tolerable. You may decide that the cost of a control far exceeds its potential effectiveness and choose not to implement it. For example, you might have a redundant data center and regular system backups but you choose to accept the risk that someone will intentionally destroy all your redundant sites at once. You may choose to accept the risk that the Federal monetary system will be destroyed because you can add no effective controls yourself. You may choose not to worry about snow preventing your employees from coming to work in Phoenix, AZ, because it is so unlikely to happen. You may choose not to provide alternative work sites for branch staff because one branch being out of service for a few days due to a flooded building is an acceptable risk. Residual risk, at least for risks you have rated high, should be explicitly acknowledged by executive management, so that it is evident that the risk has been considered in relation to the activity.

I think you can see that whatever your project or activity, risk management in the form of an independent assessment of the risks, is probably a good idea.

Risk Assessments and Great Ideas

What brings me to discuss risk management in conjunction with privacy and information security? You may have noticed the series of articles about how in early August 2006, AOL released the contents of a huge number of searches by gathering the data and posting it on the Internet. Please see Declan McCullagh's **article** on some ramifications of the incident, including the contents of some of the searches.

It appears to me (I do not have direct knowledge of this project) that the project had an excellent goal: help the corporate bottom line with a product that could answer questions about how people use the AOL search service, using data that was already present in operating the service. Usage patterns and query structures over time can help create any number of valuable results, from better products available to customers to faster, more accurate results from the search engines themselves. It can even help AOL better plan for its target demographic, by knowing what things interest their customers and what products they are hunting for. I am sure you can come up with a number of questions you would like to ask of such a large body of data.

Unfortunately, that search query data also became information (that is, had more meaning) when you looked at it in relation to specific users. In looking at the queries of particular (but not named) users, you can determine quite a lot about their current worries. Sometimes, of course, you can determine their names. Who among us has not entered our own name into a search?

Murphy (the guy with the Law) had a good time with this project, didn't he? It appears that the *transactional risk* was mitigated well. The data was gathered, information that directly identified the individuals was stripped away, the data set was certainly large enough to be statistically significant, it was successfully placed online and people certainly found it. However, when reading search queries in sequence allows one to identify a small geographic locality in conjunction with other very specific items of interest, individuals can be identified. In some cases that might be embarrassing. In other cases, it might be harmful. And in others, the identity of the searcher might simply be interesting. Would you want to know which of your co-workers was seeking help for depression? Should you know that?

In thinking about *strategic risk*, it is hard for me to see where the search query research product fit into the overall corporate strategy and priorities. Strategy and priorities are insider information (and they should be) but on the surface, it doesn't seem a really good fit. Exposing the customer base to all and sundry is probably not their first line of business.

Compliance risk does seem to be a problem. AOL has a **privacy promise**. It includes the statement about choices in information sharing, including some statements about not sharing 'network information' with third parties and that shared information will not be able to identify the user. It would seem (and I am not a regulator, but simply stating my opinion) that posting search strings would not be compliant with that promise. And that is where any of us can get into trouble.

The incident may lead to some sort of investigation by the Federal Trade Commission. It certainly led to articles that damage the reputation of AOL, thus bringing in *reputation risk*. The amount of resulting damage will not be clear for some time. Already though, Congressman Markey has proposed **legislation** to forbid websites to "warehouse" data "that is obsolete and no longer necessary for a legitimate business purpose or requested pursuant to court orders." I would hate to have to write the regulations implementing that law. What is a legitimate business purpose? How would I know what might be requested by court order sometime in the future? How do I

reconcile that with the requirements of the EU to keep data for a specific period of time? Help?

Would "Conflict" have helped? How does what happened at AOL relate back to adversarial situations? It would have been interesting to see what kind of risk assessment process was performed for this project. In doing a risk assessment, good risk managers would have asked all those tough questions. Some of the questions would have sounded to the project team like negative feedback. (Sometimes risk managers are seen as the 'sales prevention' department.) This is where understanding that sometimes conflict – encountering people with differing ideas from your own – is in your own best interest.

I would like to think that a good risk assessment would have led to a more careful review of what someone could "see" if a human looked at the data. I would like to think that the assessment would have compared the activity to the privacy policy. I would like to think that someone would have thought about the **OECD's privacy principles**: limitation of collection, accuracy and relevancy of data collected, that the data was collected for what you specified (or vice versa that you specified why you are collecting it), that you don't release it unless you have said you were going to do that; that you will safeguard the collected data so that it is not disclosed or modified or…I would like to think that the risk manager would have suggested some good alternatives (controls). Someone looking at the whole thing from a differing viewpoint might have saved AOL a lot of grief.

With all that said, I want you to understand that it is unlikely that AOL's researchers are evil. I suspect they were caught in the throes of an 'excellent idea' and no one said "wait, we might have problem here." Or, perhaps their risk assessment found a small likelihood that anyone would ever be able to connect queries with individual users to this extent, and so the project went forward. We will probably never know.

The important thing is that we learn to ask someone with that other viewpoint, someone who is likely to point out what they see as risks, onto the team to help us before we go ahead with any project. The more we calculate the risks and take steps to mitigate them, the better service we give our customers, clients, and our employers — even if it does mean the occasional passionate debate — the reasonable squaring off of adversaries.

This entry was posted in Uncategorized by **Editor**. Bookmark the **permalink [http://bcis.pacificu.edu/interface/?p=3274]** .