

WHY IDENTITY MANAGEMENT PROJECTS STALL, GO OVER BUDGET, UNDER-DELIVER, CAUSE EMBARRASSMENT OR FAIL

A White Paper

Author: Guy Huntington, President, Huntington Ventures Ltd.

Date: February 21, 2009

Table of Contents

Why Identity Management Projects Stall, Go over Budget, Under-deliver, Cause Embarrassment or Fail..... 3

 Why do identity management projects stall, go over budget, under-deliver, cause embarrassment or fail?..... 3

 Identity Management is a Process! Not Technology or a Software Product!.....4

 Don't Sell Security – Sell Business Benefits to the Non-IT Departments4

 Set you long-term goals wide and then create a strategy with a series of very tightly scoped mini-projects 5

 Operations7

 Scaling.....8

 Using Large Consulting Companies and Off-Shore Implementation Vendors 9

 Conclusion10

 About the Author10

WHY IDENTITY MANAGEMENT PROJECTS STALL, GO OVER BUDGET, UNDER-DELIVER, CAUSE EMBARRASSMENT OR FAIL

Advisory firms like Burton Group and Gartner all can tell you that many identity projects stall, are over budget, under-deliver or fail. If you're just starting out on an identity management project, this is good. You can learn from many of the past mistakes of other enterprises that have gone before you.

I'm a very experienced independent identity management consultant who has rescued several large Fortune 500 identity management projects. So I speak from much experience. This paper is designed to alert senior management on the pitfalls as well as to tell them how to structure an identity management program or project that succeeds, meets budgets, scales after the implementation consultants leave and is highly available all the time.

Why do identity management projects stall, go over budget, under-deliver, cause embarrassment or fail?

It's been my experience that there are many reasons. Usually there is a combination of factors in achieving the above:

- IT is running the project
- It's a security project
- Scope creep
- CFO was sold a bill of goods on ROI that isn't achievable
- Lack of enterprise sustained buy-in, especially by senior management
- Belief that the "vendor" will solve all the problems
- Belief that the large "implementation consultants" will solve all the problems
- No idea on the operational impact to the enterprise infrastructure
- Lack of preparation on business processes

In this paper, as I go through the key components of a successful identity project, I will give examples in my past experiences where the above occurred to illustrate the price that is paid for not doing so.

Identity Management is a Process! Not Technology or a Software Product!

The first key to success is recognizing that identity management is a process and not technology or a software product. IT loves technology. They also have their favourite vendors. They are usually in control of an identity project. This is the route to disaster. Why?

Who owns the identities in an enterprise? It certainly isn't IT. HR often owns employee identities. They may or may not own contractors, third parties, students and temps. These are often owned by Purchasing or Finance. Business partners are often owned by Finance. Customers are owned by Marketing. Facilities often own identities such as suppliers who come through their physical security systems that they manage.

When I walk into an identity management meeting for the first time to rescue or lead a project, the first thing I do is look around the table. If I only see the CIO, VP IT and their underlings, then I know right away that IT is running the show and it won't work.

Identity management is all about streamlining identity business processes that the other departments initiate, control role changes and determine terminations. All too often I find that IT is focussing on the technology and software while assuming that either the implementation consultants or the other departments will figure the processes out as an appendage to the project. I've even seen RFP's that say this!

My first advice is to get the other business units on-side and do your homework before getting to the RFP and vendor selection stage.

Don't Sell Security – Sell Business Benefits to the Non-IT Departments

When IT talks they usually talk “mumbo-jumbo” or “technoid” to the other business units. They talk about software, technology and security, which the other business units either don't want to listen to or prioritize down their list given the business objectives they want to achieve.

Several times in the past, I have stopped an identity project and then spent a couple of months working with HR, Purchasing, Finance, Marketing and Facilities to get them on-side at senior and middle-management levels for an identity project. This is the hardest part of an identity project.

I talk to HR about things like employee and worker self-serve, streamlining their onerous workflows, helping HR regain control of their employee processes like role changes, putting HR in control of worker certification and training before allowing the identity access to critical areas, improving the user experience in intranets by customizing information for them, integrating their benefits suppliers directly into the intranet eliminating uids and passwords the employee has to remember, etc.

With Purchasing, I talk about their desire to reduce inventory management and reduce costs by going to a just in time inventory system. This leads to a discussion of web services and vendor applications that will query their inventory and asset management systems. I then point out that

these are all identities too. I also talk about their time consuming tasks of dealing with suppliers and contractors. I show them how we can streamline them and ensure things like background checks are done.

For Marketing, I talk about things like being able to cross-sell to customers more effectively, tailoring each cross-sell to the individual customer. I explain how we can improve the online customer experience by eliminating numerous passwords and the ability to use different authentication methods such as biometrics etc.

For Facilities, I talk to them about reducing their operating costs for running the physical badging systems. I discuss with them how to streamline workflows for people who are visiting or using the facilities.

For all the above, I rarely talk about security directly. I then end the conversations by saying that “oh by the way, you get improved security as well”.

For senior management like the CFO, CEO, COO and CSO I talk about reducing overall regulatory reporting costs, matching security against business risk, reducing operating costs by integrating physical and logical security, increasing sales, faster partnership connections when they decide to outsource etc.

Do your homework! Don't talk about vendors and technology. Sell the business benefits and line up senior and middle management to support the project. Let them know a realistic timeframe for implementation (normally 2-3 years). Tell them you need them to be there for you when the project is underway and you're getting road blocked by departments or managers.

Set you long-term goals wide and then create a strategy with a series of very tightly scoped mini-projects

Senior management needs to understand the long-term strategy for identity management. It can help transform the enterprise to a quickly changing enterprise if implemented properly. I try to set in the senior management's minds the following key areas identity management can assist them in:

- Quick on and off boarding of all identities
- Ability to quickly form partnerships and/or out-source
- Improve security around high value risk areas both physically and logically
- Reduce long term operating costs by leveraging web services
- Happier customers and workers when interacting electronically with the enterprise
- Reduce risk of cyber and physical attacks against the enterprise

After getting the other business units to buy-in, creation of the strategy is the second most important part of an identity project. I have often found that the lead managers and their consultants don't set out a well thought out roadmap. Too often they are leaping to deployment strategies without laying in the plan for the following:

1. **Getting all the business units to sit around the same table and work out all identity management processes for creating the identity, doing role changes or extensions and voluntary and involuntary terminations** – this can take up to a year to achieve in some enterprises.
2. Determining what systems will be the authoritative sources for the different identity types. This is particularly hard when physical security systems are considered. At two enterprises, it took me over a year to get HR to agree that all non-customer identities would be placed in the ERP with ownership by HR and delegated management to Purchasing, Facilities, etc.
3. Determining the ability of the authoritative sources to interface with the enterprise directory or directories. If the enterprise has old ERP's or other applications, then time and money needs to be allocated for designing the interface.
4. Determining the legal changes to things like vendor, contractor and third party contracts – I have often found that this can take over a year to achieve.
5. Examining the operational infrastructure requirements – this is much more than the identity management servers (read the ops section in this paper for more information). I have frequently found that this can take up to a year to implement.
6. Determining which apps will be on the list for single sign on, provisioning and web services for the first release, the next release and then over the next three years (see the scaling section of this paper for more information).
7. From all the above determining realistic timeframes for requirements gathering, design, build and test, implementation, maintenance and expansion.
8. Determining realistic budgets and ROI's based on the above.

When you have this done, then you need to set very tight scope steps or projects. For example, at one customer I created an identity management program with eight projects within it. For each project I then created very tight scope requirements and kept the implementation teams on track and didn't allow scope creep.

Operations

Before you get to the vendor selection stage, you need to consider the infrastructure, org chart and operational requirements from an identity management project. It has been my own experience that SSO (single sign on) and in some cases provisioning systems need to be at 99.999% availability. In the past, at two enterprises, the enterprise disagreed with me saying that best efforts would suffice and that senior management had signed off on it. I disagreed telling them that if their SSO system went down, I thought the CEO would be calling them.

One enterprise went down for six hours. The CEO was on the phone every 30 minutes demanding to know when it would be back on line since the enterprise had ground to a digital halt. The other enterprise lost their main data centre for 48 hours and didn't have hot-failovers I had recommended.

You, the reader, should be a little scared reading this. The identity management system crosses over most of your internal infrastructure. The user, using their browser, attempts to launch an application. The request travels over the network to the app server where the signal is intercepted and redirected through the network, behind an internal firewall and load balancers, to the identity and access management sub-net. The request goes to an access server which talks to the directory server and then authenticates, authorizes and audits the identity. The request is then sent to the app server.

If your system is going to be up at 99.999%, this means that all points in the journey need to be monitored, at least every minute. The monitoring system needs to take all these points and then to automatically escalate them given the situation. There needs to be one person or group of persons who can instantly understand and respond appropriately.

In most enterprises I have worked in, achieving this usually results in re-orgs. It requires a security ops centre where the personnel are cross-trained on network, database, security, LDAP servers, firewalls, load balancers and app servers. You don't have hours to figure things or to call for someone for advice when you're running at 99.999%. You have seconds and minutes.

I have frequently worked across all of IT and their different IT business units to create this. It usually means integrating with ITIL apps like Remedy and many different monitoring systems. Further, given the increasing integration between physical and logical security (read my white paper on this), it places additional requirements to create a unified security ops command centre and console.

At many enterprises, I have created a project just to provide high availability. This normally takes several months to a year to create.

Scaling

I have frequently come into an identity management project where the implementation consultants had left and the CFO and the CIO were mad because the business benefits weren't realized. While blame was put on the implementation consultants, I often found it was because senior management hadn't done their homework. Instead they thought the software and the implementation consultants would somehow magically scale the project after implementation.

In one project, I had to design a system that would integrate SSO for 1,500 applications across 15 different business units. I created a sub-project that addressed scaling. My goal was to design business processes, that all business units would buy into, that would rapidly lead to integration for most apps and where the enterprise employees would in the end do most of the work themselves.

That's what we did. The enterprise decided to integrate about 500 apps a year. Three years later, all 1,500 apps were successfully integrated.

Note that I said business processes and not technology as my goals. I wanted to have agreed upon business processes where each business unit CIO, their managers and app owners would agree to. We had educational PowerPoint's and Word documents put on line describing to them the overall process as well as the technology implications. They then filled in on-line forms which went to a group of analysts.

The analysts would quickly categorize the app based on the agreement we had reached with the business units. It would then go into one of four categories, for which we had business processes in place to deal with them.

The app owner would then be directed to our Dev environment. The app owner had to sign an agreement stating what kind of testing they would do in Dev and Test and things they would not do. They were then migrated to Pre-prod and then into Prod.

I have used the same model in Provisioning. All of this requires lots of thought and preparation with different people in your business units. As well, the implementation consultants need to train your personnel on how to do this. I have also used out-sourcers to do portions of this.

When you talk to enterprises that say they use SSO or provisioning, ask them how many apps they have in the enterprise and how many they have integrated? You will often find that they have done less than a hundred apps and that they have over a thousand apps in the enterprise. If so, then ask them what their plans are for integrating the rest? Frequently you will not be given a direct answer because the enterprise doesn't have a plan to do this with budget and resources assigned.

Using Large Consulting Companies and Off-Shore Implementation Vendors

Frequently I have found that my past clients used large consulting firms unsuccessfully. This was not always the fault of the consulting firms. The scope for what the consulting firms was brought in to do was not sufficient for having a successful project.

For example, if IT is issuing the contract, they often don't spell out that HR, Purchasing, Finance, Marketing and Facility aren't all on-board. The implementation consultants arrive to slowly figure this out. Several months later, the project is delayed, goes over budget and under delivers.

I have found that the best way to use large consulting firms is to first of all have most of your homework done internally or by using a specialized consultant like myself. We can see the pitfalls on the road ahead before they occur and create a strategy, budget and timeline that will address all the potential problems. A lot of internal politicking needs to go on first before bringing in the fleets of implementation consultants.

Secondly, I strongly recommend that the RFP and contract issued to the large consulting companies be extremely detailed. I have numerous requirements documents attached to the RFP so that implementation bidders can understand exactly what they are getting into. In one RFP worth several million dollars spread over three year, the two lead bidders were \$100,000 apart. They bid knowing exactly what the work was.

I have worked on several projects where off-shore vendors were used. One was very frustrating to work with because of how the contract was designed and how the project manager managed it. On two other projects, I have successfully worked with off-shore vendors.

How you select the off-shore vendor, manage them and integrate them with your identity team is all critical to having a successful project. I carefully recommend to my clients off-shore vendors to use. Then I design the contracts carefully, and often lead the daily team meetings with the off-shore vendor on the line reporting daily progress. If you do this, you'll be successful at a lower cost than using all on-shore, more expensive resources.

Conclusion

If you've made it this far in the paper, than by now you should realize that identity management projects are complicated. It crosses over almost all departments, involves rethinking business processes, requires on-going co-operation of business units, requires a significant infrastructure and greatly affects security. Therefore, doing your homework before starting out on an identity management project is critical to your success.

I have seen CIO's fired over a failed identity project. You should also understand that by doing your homework up front, that you can and will have a successful identity management project.

My last advice to you is to not let the "technoids" run your identity project. Have the business units in the driver's seat at all time. Then bring in the technical people.

About the Author

Guy Huntington, President of Huntington Ventures Ltd., has lead, rescued, architected and been the program and project manager for a number of Fortune 500 identity projects including Boeing, Capital One and Kaiser Permanente. He has worked with a number of different identity management vendors' products; designed RFP's and brought in large consulting companies and off-shore vendors. Guy has extensive experience integrating physical and logical access systems. He is also currently working on a proposal to further integrated identity and content management.

Guy can be reached at: guy.huntington@hvl.net; 604-861-6804 (cell) or www.authenticationworld.com.