

Win in the flat world

Extracting Value in Information Security Services through IT Service Management

– Ramshankar Ramdattan

Background

Information Security is an absolute necessity in today's information-dependent environment. We all understand this fact, especially given the numerous threats that are prevalent out in the open, ranging from viruses to terrorism. However, organizations still view Information Security as a cost whose value is not clearly understood. Typically the true value of Information Security is understood only when a real calamity strikes.

However, if the various components that comprise an end-to-end Information Security program can be viewed as services, and if IT Service Management best practices can be applied to these services, it changes stakeholders' outlook to a major extent.

Through our multiple consulting assignments, with large Fortune 1000 organizations, we have come to the conclusion that adopting a service-oriented approach will provide good value to stakeholders from the corporate and Information Security domains.

In this paper, we explore a standard IT Security service and try to outline how we can achieve the above objectives.

This paper was presented at the "Pragmatic Service Management" conference, an itSMF event in Brighton, U.K in November, 2005.)



Before we get into that let me tell you a story. On a recent flight into London I struck up a conversation with a fellow passenger from Denver. He was talking about his hotel experiences. Many years back, he and his wife were on their first honeymoon and they checked into a prominent hotel at a ski resort.

As part of the checking-in process, they were escorted into a room where there were many closed and numbered shelves.

The person from the reception went over to a number of shelves and produced six large-size keys. This is what he said - "Key # 1 is for your room, key # 2 is for the balcony, key # 3 is for the main hotel door, key # 4 is for the heated pool area, key # 5 is for the left-side door to the hotel, and key # 6 was the duplicate of key # 1 (your room key)."

To top it all, guess what the fine was for losing a key? It was 50% of the room rent.

As you may imagine, one of the things that this couple did during their holiday was check their keys all the time. To say nothing about how bulky they were, sticking out of their pockets and poking them everywhere.

Luckily for us, these days, we don't have so many keys to carry around. We just have a single key fob which is a small rectangular card of proportions that can easily fit into a standard wallet. This provides us with central access to all needed areas of a hotel.

Friends, this is an example of a successful Single Sign-On technology in the real world. And that's the IT security service we are going to talk about, but in the virtual or the electronic world, for sign-on into enterprise applications.

We first try to understand the role of this Central Gatekeeper, the organization behind the service, the relevance of IT Service Management to this service, some of our key observations, and the value areas from our Service Management journey.

Key Drivers for Single Sign-On Security Services

So how did all this come about? Looking back at the hotel scenario, do you think the couple would visit the hotel again? Probably not. Similarly, in the virtual world stakeholders need more empowerment, organizations want to lower the cost of building username/ password code into each and every application, and lower the helpdesk cost in resetting passwords.

How many applications does the average large corporation have? 50-100? No, it is probably around 500. You know that! But whatever that number, from a user's perspective the burden of storing usernames and passwords in his or her head is cumbersome and inefficient.

So, above all, there is the need to increase end-user productivity.

How the Service Works

How does this service work? To start with, users need access to common business applications as in Financial, Human Resources, and Marketing. SSO security services enable them to get to that goal.

In a simple configuration, users first pass through the first layer of sign-on where the access request is submitted to a web proxy or a web agent sitting on a web server, and then this is forwarded to the second layer where the authorization is completed. In the third layer, the exact rights that the user has to the particular application is provided and users gain access to secured applications to complete the picture.

The Organization behind the service

So who is typically behind this program? Who are the owners? A suggested view into how the organization is architected will start with the Chief Information Security Office –Program Management office at the top and the rest of the organization within the various phases of Pre-Integration, Analysis, Design, Build, Test, Deploy, Prioritize, and Support. The service owners may be from the role that heads the integration team and the support team or a combination of both.

Operations and Challenges

There is significant complexity in the process of moving an application from SSO Integration to SSO Support.

This opens up several challenges and the following is a summation of the same.

- 1) First is a project-centric mindset. Once the application is integrated it is a regular run-of-the-mill job to support the outcome? No it's not! It is the end of the project and the beginning of the service. In fact, every new integration project increases the scope and capability requirements of the SSO Support service.
- 2) Second, there are multiple vendors managing infrastructure services on which SSO depends, which brings in the need to coordinate with multiple stakeholders to take care of issues.
- 3) Third, there is no true understanding of the service dependencies.
- 4) There may exist a negative end-user perception on availability (can you hear those voices — “I can't access that application; it must be SSO!”; “Oh, today the marketing app. is slow; must be SSO!”).
- 5) And, above all, the lack of recognition or awareness of this core IT security service

The ITSM connection

So what do we do in such a scenario? This underscores the need for an important Service Management initiative with a clear objective, scope and defined results.

From an approach perspective, it really boils down to:

- a) Undertaking an environment understanding
- b) Modeling the Service Dependencies
- c) Conducting an ITIL based service assessment
- d) And generating a Service Catalog for the support utility

With the overall objectives leading to:

- a) Align SSO services to the industry standard ITSM framework
- b) Institutionalize Service Management practices across the service portfolio
- c) Enhance service control, delivery capabilities and the overall efficiency

Certain ITIL processes have much more relevance to Single Sign-On services as compared to other processes.

We can see good linkages from an operational standpoint to Change, Configuration and Release Management, whereas from a strategic standpoint, there is the emphasis on Availability, Capacity, Security and IT Service Continuity Management. Security Management and Service Desk are two central linkages that go across the SSO service.

A mapping of the individual processes provides a deeper detail on the importance of IT Service Management. This kind of mapping will help us to understand what processes need to be adopted at every stage in the journey.

Observations from a typical ITIL Assessment

Back to the hotel story – Obviously the hotel director soon found out that honeymoon couples were no longer coming in. So what did he do?

Go on his own honeymoon to another hotel to find out the difference!

And conduct an Assessment. Let us take the same back into the SSO program and see what came out of an ITIL-based assessment.

Release Management process is not viewed as a priority due to lack of recognition of the criticality of the SSO service. However, on the positive side, change calls are usually scheduled, back out notifications received, and release packets used.

But there are some challenges starting with:

- 1) Overlapping of responsibilities between Change and Release Management
- 2) The lack of a formal acceptance post-change

As seen from this and other observations, from a Release perspective SSO is flying below the radar (it has low recognition) and due to this there is a lack of priority for release steps of the SSO service.

From the perspective of Service Level Management, Service Levels are reported and published. However, there are limited SLA terms and subjective prioritization criteria for integrated applications.

From this stems our view that Service Level terms need to be elaborated in more detail since there is a lack of understanding on the dependencies associated with peripheral services.

What about availability? From an Availability perspective, it is important to understand that Single Sign-On is really a “sandwiched” service - between Network and Server Infrastructure.

In this particular scenario, external suppliers provide Network Services (one) and Infrastructure Services (Server Management, Database Management, etc.) (two) to Business Users and applications.

Single Sign-On Services engage these entities via specific service request tools and provide direct availability service levels to business critical applications. However, the SSO Service Availability is directly dependent on the availability levels of the Infrastructure and Network services.

Our observation in this area is that Availability Management will be challenging in a scenario where multiple service providers have independent availability targets. Service partners do have their own service levels as mandated by contracts with defined owners and responsibilities.

However, availability service expectations from the Line of Business owners need to be periodically refreshed and having a service catalog will facilitate better discussions.

Five key value propositions

So how did our infamous hotel do? They woke up and so did we in the virtual world, which resulted in a few key recommendations.

Which brings us back to the title, “How do you extract value from this information security service?” By focusing on our five key value propositions, as below:

People: The people area is really key and boils down to three main points —

1. Participation: Get everyone involved. Understand that SSO is a sandwiched service, so get all relevant stakeholders in your boat.
2. Awareness: Increase the level of awareness, amongst business partners and technology owners. Make them dependency aware. Conduct a few workshops to communicate this.
3. Understanding: SSO teams need to be aware of the direct and indirect impacts after knowing the inter-service dependencies

In the process area -

1. Make folks ITIL-aware. Start with Configuration, Change and Release in phase 1 and then go on to Availability, Capacity and Service Level Management.
2. Derive a dependency model amongst processes, process owners, and spans of authority and responsibility.
3. Use Service Catalog as a communication vehicle and to highlight key metrics.

Within the Technology area -

1. Design the architecture to facilitate segregation of services – What this means is that higher priority business applications, e.g., financial reporting or SOX applications and customer facing applications, are provided a separate SSO service (instead of clubbing the entire service into one).
Using a “one size fits all” approach for all applications may not be helpful as any issue with the SSO service can have a severe impact on the business in terms of application downtime.
2. Ensure that all technology owners (especially Infrastructure, Network and Single Sign-On) regularly communicate on what’s going on, simply because a change in any one area could have an impact on the SSO service.
3. Deploy technology that provides for a good scalability and caters to capacity growth. E.g. A new integration could suddenly introduce more users or the same users doing more things post sign-on.

What about Security -

1. Realize that Single Sign-On’s greatest benefit is also its greatest downside, since it represents the single point of entry into multiple applications. Architect the utility keeping this security aspect in mind. Use distributed components to support prioritized application tiers so as to maintain a redundancy in the security strategy.
2. Access Control/ Management – Complement Access Management efforts by providing the right access to the right users and reporting for user access review and audit operations.
3. The Service should also be able to complement requirements for session logging, access tracking, and reporting on the service conditions

Known Pitfalls

No initiative is without its challenges, so watch where you are going and watch out for specific issues.

The two biggest areas to look out for are the existing Vendor contracts and business, as usual, requirements. To introduce enhancements, a practitioner needs to navigate through these areas first. After that, there are the following:

- 1) The tendency to view Service Management as an external initiative and not internal to the SSO service. Service owners' and service personnel's involvement is critical to make this a success.
- 2) The lack of an up-to-date expectations summary from Business Partners. Try to capture these again if Service expectations are over a year old
- 3) Due to the varied nature of the stakeholders (coming from multiple service partners) there may be conflicts on what constitutes Critical Success Factors.
- 4) Application downtime is always attributed to Single Sign-On services, which is really a perception issue, and this needs to be changed (over a period of time) by effective reporting on the root cause of the downtime and conducting communication workshops.
- 5) Again, due to the presence of multiple service partners, each partner may have their own service definitions and functionalities. Create a common statement of service definitions and ensure partner alignment towards the same.

Conclusion

To conclude, remember that Single Sign-On services will continue to play a critical role in organizations' endeavor to perfect Identity and Access Management services.

Ensure that process stakeholders participate and have relevant empowerment to succeed in this area.

Stress the importance of using Service Management processes and the ITIL framework within the internal processes of the SSO utility.

Conduct a service test bed with a few critical business applications and use the results to drive changes in other applications/ service areas.

Use Service Catalog as a vehicle for communications within and outside the utility.

And finally, provide for an ample timeline to reach the milestones of the SSO Service Management journey. Have patience! The results will speak for themselves.

About the Author:

Ramshankar Ramdattan is a Senior Consultant with Infosys Technologies. He has over 10 years of industry experience covering process consulting, project management and information security management. In his current role, he consults with the Information Protection Management group at a Fortune 100 organization.

This paper was presented at the "Pragmatic Service Management" conference, an itSMF event in Brighton, U.K in November, 2005.)

© 2005 Infosys Technologies Limited.

ALL RIGHTS RESERVED

Copyright in whole and in part of this document "**Extracting Value in Information Security Services through IT Service Management**" belongs to Infosys Technologies Limited. This work may not be used, sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or in any media without the prior written consent of Infosys Technologies Limited.